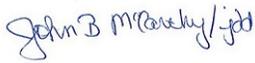


APPOINTING AUTHORITY APPROVAL 	POLICY NUMBER ODM-IPP 3922 VERSION 1
	EFFECTIVE DATE: July 6, 2015

I. PURPOSE:

- A. To inform all Ohio Department of Medicaid (ODM) employees, contractors, business associates, external agencies and county employees of their responsibility for maintaining the confidentiality and security of all personal information to which they have access in the course of performing their duties.
- B. To provide instruction relating to the procedures for the user of the revised form ODM 07078 – Ohio Department of Medicaid Code of Responsibility (Appendix A). The ODM 07078 form describes the specific information and confidentiality requirements to which all ODM system users including ODM employees, contractors, business associates, external agencies and county employees must subscribe in order to gain access to ODM and specific State of Ohio systems.

II. REFERENCE/AUTHORITY:

A. REFERENCES

1. Information Technology Policy ITP E.8, Use of Internet, E-mail and Other IT Resources, published by The Ohio Department of Administrative Services, dated March 19, 2008.
2. Internal Revenue Code, Section 7213 (a).
3. Ohio Revised Code (ORC) [5160.03](#), [5101.27](#) through [5101.31](#), [5101.99](#), [3107.17](#), [3107.42](#), [3107.99](#), [3121.894](#), [3121.899](#), [3121.99](#), [3125.08](#), [3125.50](#), [3125.99](#), 1347.15, [4141.21](#), [4141.22](#) and [4141.99](#)
4. Code of Federal Regulations: 45 CFR 160 and 164 (HIPAA-45 CFR164.501); 42 CFR 431.300 through 431.307; 5 USC 552a; 7 CFR 272.1(c)
5. Ohio Administrative Code (OAC) rules [4141-43-01](#) through
6. [4141-43-03 IPP 3001 ODM Information Security](#)
7. [IPP10002 Computer Usage and Information System Usage](#)
8. [IPP 3925 ODM Data Access Policy](#)
9. [IPP 10004 Incident Reporting](#)
10. [IPP 8106 Research and Research Data Approval](#)

B. AUTHORITY

This policy is established by order of the Director, ODM, hereinafter referred to as Director. Per ORC 5160.03, all duties conferred on the various work units of the department by law or by order of the Director shall be performed under such rules as the Director prescribes and shall be under the Director's control.

III. SCOPE:

This procedure applies to all ODM system users including ODM employees, contractors, business associates, external agencies and county employees as noted in Section I.A. of this policy.

IV. DEFINITIONS:

- A. SYSTEM ACCESS MANAGEMENT – Identifies the section within ODM responsible for granting, requesting, provisioning, de-provisioning and/or revoking access to systems under the control of ODM.
- B. AUTHORITATIVE SOURCE – An ODM employee(s) with responsibility to authorize access for an external entity user(s), identify the level of access required, submit a formal request on behalf of the external entity user(s), and provide notice of access termination to ODM System Access Management.
- C. SUPERVISOR – An ODM employee(s) who has the responsibility to identify internal employees with the need to access the system, identify the level of access required, submit a formal request, and provide notice of access termination to ODM System Access Management.
- D. PROGRAM/DATA OWNER – The area identified as being responsible for authorizing entity(s) and level of access to a specific system and/or data. The Program/Data Owner is accountable for authorizing access to the data under their control.

V. POLICY:

- A. All individuals requesting ODM system access must complete the ODM 07078 Code of Responsibility form. The form must be signed by the requestor, their supervisor and the entities' designated Authoritative Source or in the case of an ODM employee their supervisor. Completed forms may be submitted to ODM System Access Management at accessrequest@medicaid.ohio.gov . The form serves several purposes:
 - 1. It provides a statement of understanding concerning the confidentiality and security of data and the acknowledgment of that statement by the individual.
 - 2. The form is used to establish or change access to specific ODM or State of Ohio systems for ODM system users (as noted in Section I.A.).
- B. Any access to information about recipients of ODM benefits or services, or about ODM employees, that is collected and maintained on ODM or state computer systems

is strictly limited to those purposes authorized by ODM, and as directly related to the system user's official job duties and work assignments for, and on behalf of, ODM and/or a federal oversight agency.

- C. The ODM 07078 form must be completed by all ODM employees when hired. Completion of the form will be facilitated by ODM Human Resources.
- D. System requests, including modifications to existing access, must be submitted using the ODM 07078 and be completed by the appropriate Authoritative Source or in the case of an ODM employee their supervisor. Completed forms are to be sent to ODM System Access Management at accessrequest@medicaid.ohio.gov.
- E. The responsibility for forwarding completed ODM 07078 forms for all non-ODM employees is the responsibility of the requesting entities' Authoritative Source. ODM employee requests for system access must be submitted by their supervisor. Requests for modifications of existing system access must be accompanied by a new ODM 07078 form with approval from the appropriate Authoritative Source or in the case of an ODM employee their supervisor.
- F. If a specific copy of a completed and approved ODM 07078 form is needed, it may be requested through ODM System Access Management.

VI. CONTACT:

Please direct all questions or concerns to IPP_ODM_Policy_Admin@medicaid.ohio.gov. This Policy supersedes any previously issued directive or policy and will remain effective until cancelled or superseded.

VII. APPENDIX:

- A. ODM 07078 Code of Responsibility

VIII. REVISION HISTORY:

Date	Description of Change
	Original

APPOINTING AUTHORITY APPROVAL <i>John B. Mearns/jbt</i>	POLICY NUMBER: ODM-IPP 10002 VERSION 1
	EFFECTIVE DATE: July 1, 2015

I. PURPOSE/REASON:

To inform all ODM employees, temporary service personnel, and contractors of the proper use of ODM electronic equipment and information systems including but not limited to computers, peripherals, software, Internet, e-mail, Short Message Service (SMS) Text Messaging, Portable Computing Devices and Instant Messenger (IM).

II. REFERENCE/AUTHORITY:

A. REFERENCES

1. ODM-IPP 3922 Code of Responsibility
2. ODM-IPP 0003 Standards of Employee Conduct
3. ODM-IPP 9002 Employment Discrimination and Sexual Harassment Prevention
4. ODM-IPP 10003 Workplace Violence Prevention
5. ODM-IPP 8501 Accounting for Protected Health Information Disclosures
6. ODM-IPP 3100 Telephone Usage
7. Ohio Revised Code 4511.204

B. AUTHORITY

1. This policy is established by order of the Director, ODM, hereinafter referred to as Director.
2. Per ORC 5160.03, all duties conferred on the various work units of the department by law or by order of the Director shall be performed under such rules as the Director prescribes and shall be under the Director's control.

III. SCOPE:

A. This policy applies to all Ohio Department of Medicaid employees, temporary service personnel, or contractors (hereinafter referred to as ODM personnel) use of computer and information systems, including but not limited to:

1. Electronic equipment-computers, computer peripherals, computer software, and laptops;
2. Information systems-documents, recordings, e-mail, Instant Messenger (IM), and the Internet; and
3. Other data contained in or recoverable from such electronic equipment and information systems.

- B. This applies to any equipment either provided by ODM or used on ODM property for ODM business purposes.

IV. DEFINITIONS:

- A. BYOD (Bring Your Own Device) - BYOD refers to employees bringing their own personal device to work, whether laptop, smart phone or tablet, in order to interface to the agencies internal production networks and/or confidential information.

- B. Portable computing device - The term portable computing device as used in this document but not limited to: laptops, flash drives, notebooks, personal digital assistants (PDAs), Smart Phones (e.g.: Blackberry, iPhone, Android based phones etc.), tablet PCs (e.g.: iPad, Kindle, Nook, etc.) and any emerging technology containing a processor and/or memory that could be used to store agency data in a portable format. The security safeguards may vary by device type, but in all cases must comply with the requirements set forth in this policy.

V. POLICY:

A. GENERAL

1. ODM computers and information systems are the property of ODM. They may be used only for explicitly authorized purposes. ODM reserves the right to examine all data stored in or transmitted by its computers and systems. Without notice, the Chief Inspector's Office, ODM supervisors, deputies, and authorized management information systems staff may enter, search, monitor, track, copy, and retrieve any type of electronic file of any employee or contractor. These actions may be taken for business- purpose inquiries including, but not limited to, theft investigation, unauthorized access and/or disclosure of confidential business or proprietary information, excessive personal use of the system, or monitoring work flow and employee productivity.
2. Personnel have no rights to privacy in their use of the Internet and e-mail. Authorized designees (as referenced above) may access any files stored on or deleted from computers and information systems. When necessary, Internet, e-mail, and Instant Messenger (IM) usage patterns may be examined for work-related purposes, including situations where there is a need to investigate possible misconduct and to assure that these resources are devoted to maintaining the highest levels of productivity. The Chief Inspector's Office has the authority and ability to monitor Internet sites contacted, e-mail, and Instant Messenger (IM) usage at its own discretion or at the request of management.

3. All software installed on any ODM computer must be licensed to ODM. Personnel must receive advance approval from their deputy director and the Information and Technology Services (ITS) deputy director (or their respective designees) before adding software programs to any ODM computer. Questions regarding currently authorized software programs and/or software licensed to ODM are to be directed to the OIS deputy director or designee.
4. When making use of personally owned devices such as laptops, cellular devices and wireless tablets within ODM facilities or on ODM provided networks, users of such devices MUST adhere to all ODM policies related to computer usage and work performance. These devices are not allowed to be physically connected to the ODM production network or ODM owned devices. For example, employees should not be linking their personal cellular phones to their assigned computers or laptops even for purposes of charging the phone. ODM does allow for WiFi access to the public internet in limited facilities. When making use of these ODM provided WiFi internet services, users are responsible for ensuring their usage of such devices does not have a negative impact on their ability to meet their work related responsibilities or inhibit the ability of those around them to perform their work. For those making use of the ODM WiFi public internet service, there is no expectation of privacy for any information sent across this network, and their activity is subject to monitoring.

B. ALLOWABLE USES OF COMPUTERS AND INFORMATION SYSTEMS FOR ODM BUSINESS PURPOSES

1. Facilitating job function performance;
2. Facilitating and communicating business information within ODM and the county network;
3. Coordinating meeting locations and resources for ODM;
4. Communicating with outside organizations as required in the performance of employee job functions.

C. PROHIBITED USES OF COMPUTERS AND INFORMATION SYSTEMS INCLUDING, BUT NOT LIMITED TO, APPLICATIONS, E-MAIL, INSTANT MESSENGER (IM), SHORT MESSAGE SERVICE (SMS) TEXT MESSAGING, Portable computing device AND THE INTERNET. The following is a non-exhaustive list of prohibited uses:

1. Violating local, state, and/or federal law (See ODM-IPP 0003);
2. Harassing or disparaging others based on age, race, color, national origin, sex, sexual orientation, disability, religion, or political beliefs (See ODM-IPP 9002 and ODM-IPP 10003). Harassment and disparagement include but are not limited to slurs, obscene messages, or sexually explicit images, cartoons, or messages;

3. Threatening others;
4. Soliciting or recruiting others for commercial ventures, religious or political causes, outside organizations, or other matters which are not job related;
5. Using computers or information systems in association with the operation of any for-profit business activities or for personal gain;
6. Sabotage, e.g. intentionally disrupting network traffic or crashing the network and connecting systems or intentionally introducing a computer virus;
7. Accessing an employee's files without authorization and with no substantial business purpose;
8. Vandalizing the data of another user;
9. Forging electronic mail and Instant Messenger (IM) messages;
10. Sending chain letters;
11. Sending rude or obscene messages (e-mail or Instant Messenger (IM) should not be used to send anything that would embarrass or discredit ODM or the State of Ohio);
12. Disseminating unauthorized confidential or proprietary ODM or client documents or information or data restricted by government laws or regulations (See ODM-IPP 8501 and ODM-IPP 3922);
13. Disseminating (including printing) copyrighted materials, articles, or software in violation of copyright laws (See ODM-IPP 0003);
14. Accessing the Internet in any manner that may be disruptive, offensive to others, or harmful to morale;
15. Transmitting materials (visual, textual, or auditory) containing ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on age, race, color, national origin, gender, sexual orientation, disability, religious or political beliefs;
16. Sending or soliciting sexually-oriented messages or images;
17. Using the Internet or Instant Messenger (IM) for political activity;
18. Using the Internet to sell goods or services not job related or specifically authorized in writing by an approving authority;
19. Downloading and viewing non-work-related streaming audio or video (e.g. listening to radio stations, etc.) due to the limited bandwidth of the system;
20. Intentionally using Internet facilities to disable, impair, or overload performance of any computer system or network or to circumvent any system intended to protect the privacy or security of another user;
21. Speaking to the media or to the public within any news group or chat room on behalf of ODM if not expressly authorized to represent ODM;

22. Uploading or downloading games, viruses, copyrighted material, inappropriate graphics or picture files, illegal software, and unauthorized access attempts into any system;
23. Using electronic devices while operating a state vehicle;
24. Storing non-work, personal documents on any drive of a state-owned computer or network.

NOTE: Whether during work hours or not, these prohibitions apply at all times. Personnel cannot expect that the information they convey, create, file, or store in ODM computers and information systems will be confidential or private regardless of the employee's intent.

D. USE OF THE E-MAIL SYSTEM AND INSTANT MESSENGER (IM)

1. Official Use

- a. When using e-mail or Instant Messenger (IM), as with all written official communications, personnel are expected to display a formal, businesslike demeanor in order to reflect professionalism and credibility on ODM and themselves.
- b. Everyone is responsible and liable for the content of his or her electronic mail or message. As stated earlier, all electronic data may be accessed at any time by the Chief Inspector's Office or management for legal or business purposes.

2. Nonofficial Use

- a. Personnel may access the e-mail and Instant Messenger (IM) system for nonofficial business provided that such communication does not disrupt or interfere with official ODM business, is kept to a minimum duration and frequency, does not violate other provision of this policy and is not political in nature. Similar to telephone usage, minimal personal e-mail and Instant Messenger (IM) may be received or sent provided that no cost is incurred by ODM.

CAVEAT: Please remember that there is no expectation of privacy for anything sent by e-mail or Instant Messenger (IM) and that others can view this information at any time.

3. INTERNET ACCESS GUIDELINES:

- a. Applicability -This policy provides only guidelines to ODM personnel for Internet access. It does not supersede state or federal laws or any office policies regarding confidentiality, information dissemination, or standards of conduct.

-
- b. General Information - In our effort to enhance client service and facilitate communication among personnel, ODM provides all personnel with Internet access. Personnel Internet access accommodates basic e-mail functions, file transfer, and interactive terminal access to accomplish ODM business goals. ODM permits personnel to use and explore this technology so that everyone may become as proficient as possible in order to improve work quality and efficiency. All ODM personnel must become familiar with and acknowledge ODM policies relating to the Internet use in order to make the best use of the technology, maintain a professional environment, and protect valuable ODM and client information.
 - c. Guidelines for Incidental/Occasional Personal Internet Usage: - Generally, the Internet is to be used for work-related purposes. ODM will permit personal use of the Internet with reasonable restrictions as to the amount of time devoted to personal usage and sites visited provided such use does not adversely affect business or productivity. Incidental/occasional use is comparable to time authorized for meals and reasonable breaks during the workday and those times only should be used to attend to personal matters. ODM has the right to insist that agency Internet resources are devoted to maintaining the highest degree of productivity. Personal Internet usage is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason.

CAVEAT: Please remember incidental/occasional use is considered part of the meal and break time of personnel. Personnel are not permitted to utilize the Internet equal to meal and break times and also take their scheduled meal and breaks. Such actions will be considered excessive.

- d. Filtering by Screening Software ODM has the right and may filter and deny users Internet access to sites considered inappropriate. Although not all-inclusive, examples of inappropriate sites that may be filtered are those depicting violence/profanity, partial or full nudity, sexual activity, gross depictions, intolerance, satanic/cult images, militant/extremist images, questionable/illegal, and gambling activities.

CAVEAT: Please remember that there is no expectation for privacy for an employee's use of the Internet and that others can view this activity at any time.

E. SECURING COMPUTER EQUIPMENT AND ELECTRONIC DATA

- 1. ODM employees who are responsible for or are assigned portable computer equipment and electronic media (i.e., phone, laptops, thumb drives, external hard drives, DVD's, CD's, etc.) shall secure those items when they are not present in the office. These items routinely contain confidential and/or HIPAA information which could be compromised if lost or stolen.

2. If over-night travel is required, the computer equipment is expected to be secured in the hotel room, residence, etc. When necessary, computer equipment can be placed in the trunk of a vehicle so long as items are not visible, but the trunk and the vehicle must be locked. Leaving computer equipment on the front or back seat of a vehicle, or in any way visible, is not permitted.
3. If an ODM employee is responsible for a pool of portable equipment (e.g., equipment that is shared by many employees), the equipment shall be secured while in and out of the office. Sign-in and sign-out sheets shall be utilized to track the location of the equipment at all times. The sign in and out sheet at a minimum should include the employee's name who is using the equipment and the pick-up and return date.
4. If an employee loses a piece of equipment or it is stolen, they are required to immediately notify the ITS Customer Service Center at 614-387-6809, their supervisor, and the Chief Inspector's Office.
5. Failure to properly secure portable computer equipment and electronic data is subject to disciplinary action.

F. VIOLATIONS OF POLICY:

Violations of this policy will be reviewed on a case-by-case basis and may result in disciplinary action up to and including removal

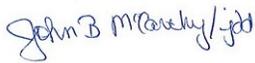
VI. CONTACT:

Please direct all questions or concerns to IPP_ODM_Policy_Admin@medicaid.ohio.gov.

This Policy supersedes any previously issued directive or policy and will remain effective until cancelled or superseded.

VII. REVISION HISTORY:

Date	Description of Change
	Original

APPOINTING AUTHORITY SIGNATURE 	POLICY NUMBER ODM IPP 3001 VERSION 1
	EFFECTIVE DATE July 7, 2015

I. PURPOSE/REASON:

- A. This policy document has been prepared by The Ohio Department of Medicaid (ODM). It is intended for use as a document of authority for managers and users in fulfilling their responsibilities for initiating, implementing and maintaining information security within ODM. It shall be used as a basis for developing departmental procedures, standards and guidelines. Physical security and contingency planning issues are addressed at a high level in this document. Contact the appropriate department for additional information, as needed.
- B. What is Information Security? - The purpose of information security is to ensure the availability of timely, accurate information to deliver products and services, while preventing and minimizing security incidents. This information, along with processing and delivery capabilities, is considered a key organizational asset and must be protected. There are three basic components of information security:
1. Confidentiality - protecting sensitive information from unauthorized disclosure or interception;
 2. Integrity - safeguarding the accuracy and completeness of information and computer software;
 3. Availability - ensuring that information is available to users when required.
- Information takes many forms. It can be stored on computers, transmitted across networks, printed out or written down on paper, and spoken in conversations. Appropriate protection shall be applied to all forms of information, including papers, databases, films, slides, models, tapes, mobile storage devices, conversations and any other methods used to convey knowledge and ideas.

- C. Why is Action Needed? - Information is considered a key asset at ODM. Maintaining the confidentiality, integrity and availability of this information are essential for maintaining accountability, legal compliance, and agency reputation. Organizations are facing increasing threats from a wide variety of sources. Thus, it is important that ODM's systems and networks be protected from threats such as: computer-based fraud, espionage, sabotage, vandalism, computer viruses, hackers and other sources of failure and disaster. These threats are expected to become more prevalent. In the meantime, ODM is becoming increasingly dependent on its Information Technology (IT) systems, networks and services. This growth presents increasing vulnerabilities, making information security policies an absolute necessity for the protection of organizational assets.
- D. Information Security Policy Statement Objective: To provide management direction and support for information security. The Ohio Department of Medicaid (ODM) relies on the availability of timely, accurate information in order to make the information-based strategy work. The information, along with processing and delivery capabilities, is considered to be a critical organization asset. All associates, temporary employees, and contractors must be responsible and accountable for protection of information to ensure its confidentiality, integrity and availability in all forms. These forms of information may include emails, files, papers, databases, slides, models, tapes, portable storage media, conversations and any other method used to convey and store information. Each departmental unit is responsible for determining the sensitivity of the data created and/or processed in that unit and establishing and/or defining appropriate controls and acceptable levels of risk. To this end, each departmental unit shall appoint a person, or persons, within the unit to act as the unit Information Security Liaison. The Information Security Liaison is responsible for ensuring that appropriate organizational security standards are developed to support the Information Security Policy. The Chief Information Security Officer is responsible for coordinating the implementation of information security measures through the agency Information Security Program, and will assist the Legal and Audit departments in providing management assurance that departmental units are in compliance with policy, legislative and contractual requirements regarding information security. State of Ohio IT Standard ITS-SEC-02, "Enterprise Security Controls Framework," specifies agencies use National Institute of Standards and Technology (NIST) Special Publication 800-53 as the framework for information security controls. The security controls specified in this policy map directly to NIST Special Publication 800-53 Revision 4. The NIST 800-53 Rev. 4 security controls for moderate-impact information systems serve as the security control baseline for ODM.

II. REFERENCES/AUTHORITY:

A. REFERENCES

1. Ohio Revised Code (ORC) 5160.03
2. ORC 1347.15
3. ORC 1347.12

4. ITS-SEC-01 Data Encryption and Cryptography
5. ITS-SEC-02 Enterprise Security Controls Framework
6. ODM IPP 3925 Data Access Policy
7. ODM IPP 3930 Periodic Access Reconciliation
8. ODM IPP 3922 Code of Responsibility
9. The Council on CyberSecurity “Critical Security Controls for Effective Cyber Defense”

B. AUTHORITY

1. This policy is established by order of the Director, ODM, hereinafter referred to as Director.
2. Per ORC 5160.03, all duties conferred on the various work units of the department by law or by order of the Director shall be performed under such rules as the Director prescribes and shall be under the Director's control.

III. SCOPE:

This IPP applies to all ODM system users (state employees, temporary service personnel, contractors, county employees, business partners, and external agencies).

IV. DEFINITIONS:

See Appendix A: IT Glossary

V. POLICY:

This policy delineates the security controls required for all ODM Information Systems. Security controls follow NIST Special Publication 800-53 Rev. 4 naming conventions and are presented according to control families. These security controls apply to all ODM Information Systems.

A. Access Control (AC)

Objective: To restrict access to a place or information technology resource. This ACCESS Control Policy and procedures reflect applicable state and federal laws, Executive Orders, directive, regulations, policies, standards, and guidance.

1. AC-2 Account Management
 - a. Authorized User Registration - Local access (from within the Ohio Department of Medicaid facility) to the system network is controlled through use of individually owned user accounts and associated confidential passwords. Remote access to the system network shall be controlled through an additional access point that utilizes individually owned tokens with dynamic passwords. Users are responsible and will be held accountable for all transactions initiated and/or completed under their

accounts, unless the user has notified the Chief Information Security Officer, via the ITS Service Desk, that the account has been compromised. Authorized user registration process includes the following:

- 1) Verifying that the user has authorization from their department's Security Liaison;
- 2) Verifying that the user has authorization from the system guardian as required;
- 3) Checking that the level of access granted is appropriate for the user's purpose and is consistent with the Information Security Policy;
- 4) Requiring users to sign a form indicating that they understand the conditions of access;
- 5) Maintaining a formal record of all persons registered to use the service;
- 6) Immediately removing the access rights of users who have changed jobs or left the organization;
- 7) Removing redundant user IDs and accounts that are no longer required;
- 8) Ensuring that redundant user IDs are not reissued to another user.

2. AC-3 Access Enforcement

- a. "Need to Know" Principle - All information Systems must enforce user access controls and authorization procedures to ensure that only authorized individuals gain access to information or systems necessary to only undertake their specific duties.
- b. Documented Access Control Policy - Organizational requirements for access control shall be defined and documented. Access requests must include a clear statement of the organizational requirements for system access in order to implement and maintain an effective level of control of access to IT services and data. Each data or application guardian shall maintain a clearly defined access policy statement which defines the access right of each user, role, or group of users and the security requirements for individual applications. Information dissemination and entitlement shall be based on the "need to know" principle. Consideration shall be given to the establishment of standard user access profiles for common categories of users. System Owners have this responsibility. Please see the ODM Data Access Policy (IPP 3925) for additional information related to this subject.
- c. Privilege Management - The use of special privileges must be restricted and controlled. For multi-user systems that requires protection against unauthorized access, the allocation of privileges will be controlled by the system owner through a formal authorization process as follows:
 - 1) Identify the privileges associated with each system product (i.e., operating system, database management system, and categories of staff to which they need to be allocated).
 - 2) Allocate privileges to individuals on a "need-to-use" basis and on an "event-by-event" basis, (i.e., the minimum required access for their functional role, only when needed.)

-
- 3) Maintain an authorization process and a record of all privileges allocated. Privileges shall not be granted until the authorization process is complete.
 - 4) Promote the development and use of system routines to avoid the need to grant privileges to users.
 - 5) Assign separate IDs for special purposes that require high privileges.
 - d. Review of User Access Rights - To maintain effective control over access to the networks and data, the ODM HIPAA Unit will conduct periodic reviews of users' access rights (see IPP 3930 Periodic Access Reconciliation). This review will ensure that:
 - 1) Users' access capabilities are reviewed for appropriateness;
 - 2) Privilege allocations are checked at regular intervals to ensure that unauthorized privileges have not been obtained.
3. AC-5 Separation of Duties
- a. Segregation of Duties - Segregation of duties minimizes the risk of negligent or deliberate system misuse. Therefore, consideration shall be given to separating the management or execution of certain duties, or areas of responsibility in order to reduce opportunities for unauthorized modification or misuse of data or services. In particular, it is recommended that the following functions are not being carried out only by a single individual:
 - 1) System use (non-technical system users);
 - 2) Data entry;
 - 3) Computer operation;
 - 4) Network management;
 - 5) System administration;
 - 6) Systems development and maintenance;
 - 7) Change management;
 - 8) Security administration;
 - 9) Security audit.
4. AC-6 Least Privilege
- a. Privilege Management -The use of special privileges must be restricted and controlled. For multi-user systems that require protection against unauthorized access, the allocation of privileges will be controlled by the system owner through a formal authorization process as follows:
 - 1) Identify the privileges associated with each system product (i.e., operating system, database management system, and the categories of staff to which they need to be allocated).
 - 2) Allocated privileges to individuals on a "need-to-use" basis and on an "event-by-event" basis, (i.e., the minimum requirement for their functional role only when needed.)
 - 3) Maintain an authorization process and a record of all privileges allocated. Privileges shall not be granted until the authorization process is complete.
 - 4) Promote the development and use of system routines to avoid the need to grant privileges to users.

-
- 5) Assign separate IDs for special purposes that require high privileges.
 - b. Use of Standard and elevated Privilege accounts for login ODM requires that each user login to their workstation with a non-administrator/root account, and to use their privileged account to "Runas" and "Sudo" for administrator access to the specific application or service only as needed or directed. Caching/saving elevated credentials in a script or other method is restricted and must be approved by the Chief Information Security Officer prior to use. Systems must prohibit non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
5. AC-7 Unsuccessful Login Attempts
 - a. Number of Unsuccessful login attempts before account lock
The number of unsuccessful login attempts allowed is five before action is taken to record the unsuccessful attempt, and lock the account.
 - b. Account Lockout Period
Locked accounts remain so until they are reset by the system administrator or by the system after 36 hours.
 6. AC-8 System Use Notification
 - a. Login Notice Warning
Each Information System shall display a general notice warning that displays to users a general notice warning/banner before being granting access to a system that contains confidential information. The privacy and security notice (general notice) shall be consistent with applicable federal and state laws, executive orders, directive, policies, regulation, standards, and guidance and state that:
 - 1) Users are accessing an ODM information system;
 - 2) Information system usage may be monitored, recorded, and subject to audit;
 - 3) Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
 - 4) Use of the information system indicates consent to monitoring and recording;
The information system shall retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.
 7. AC-11 Session Lock
 - a. Default Session Inactivity Value - Each Information System or device shall prevent further access to the system by initiating a session lock after 15 minutes of inactivity for upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication procedures. Any required deviation from this value shall be approved by the Chief Information Security Officer.
 8. AC-12 Session Termination
 - a. Session Termination conditions - Session termination ends/stops all processes associated with a user's logical session except those processes that are
-

specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination are:

- 1) Terminating a user's session after 30 minutes of inactivity.
 - 2) Targeted responses to certain types of incidents.
 - 3) Time-of-day restrictions on information system (See AC-12 (B) "Limitations of Connection Time") any required deviation from this policy shall be approved by the Chief Information Security Officer.
- b. Limitation of Connection Time - Restriction on connection times will provide additional security for high risk applications. Limiting the period during which connections are allowed to computer services reduces the window of opportunity for unauthorized access. Such a control will be considered for sensitive computer applications, especially those installed in high risk locations (i.e., public or external areas that are outside ODM's security management). Examples of such restrictions include the following:
- 1) Using predetermined time slots (i.e., for batch file transmissions or regular interactive session of short duration);
 - 2) Restricting connection times to normal office hours, if there is not requirement for overtime or extended-hours operations.
- c. Public Terminal Time-Out - Inactive terminals in high risk locations (i.e., public or external areas that are outside ODM's security management) or serving high risk systems, shall be set to time out to prevent access by unauthorized person. The time-out facility must clear the terminal screen and close both application and network sessions after a defined period of inactivity. The time-out delay must reflect the security risks of the area and the users of the terminal.
9. AC-14 Permitted Actions without Identification or Authentication
- a. Information Systems containing CPI - No ODM Information System, Application, or Service that contains, uses, or sends Confidential Personal Information (CPI), will permit a user to perform any action upon that CPI data without proper Authentication and Authorization.
10. AC-17 Remote Access
- Facilities for external connection to components of the ODM Network (PCs, routers, servers, gateways, mainframes, communications service provider access points, etc.) may provide a means of unauthorized access to applications. Connections by remote users via public or non-ODM Networks must therefore be authenticated through an additional access point that utilizes tokens with dynamic passwords. Each remote system user must come into the Network via an individually owned token account. All other forms of remote user entry into ODM's Networks are prohibited, unless an explicit exception has been granted from the Chief Information Security Officer, with the approval of IT management.
- a. Use of digital-to-analog devices that connect to desktop telephones is prohibited unless explicit exception has been granted through the Officer of Information and Technology Services

- b. No server-based functionality is permitted with dial-out lines unless used in conjunction with tokens and dynamic passwords.
ITS personnel are responsible for taking precautions to ensure that they do not participate in the establishment for maintenance of any unauthorized remote connections. ITS personnel who feel they are being pressured to violate they policy shall immediately contact their manager or Chief Information Security Officer.
ITS must maintain an inventory of all analog lines installed in ODM facilities. This inventory shall include the number and purpose of the line.

11. AC-18 Wireless Access

- a. Wireless Access to the Internal Network
ODM information must not be transmitted via wireless communications technologies unless:
 - 1) It is encrypted by a Cipher using at least a 128bit cipher key. The Algorithm/Encryption Module shall be FIPS 140-2 compliant.
 - 2) Wireless Access Points are placed in secure areas.
 - 3) A firewall is implemented between the wireless and wired network infrastructure.
 - 4) Intrusion detection agents are deployed on the wireless side of the firewall.
 - 5) MAC address authentication is utilized.
 - 6) Wireless activity is monitored and recorded, and records are reviewed on a regular basis.
 - 7) Personal Firewalls are utilized on all wireless clients.
 - 8) All Wireless Access Point installations must be approved by the Chief Information Security Officer prior to deployment.

12. AC-20 Use of External Information Systems

- a. External Facilities Management
The use of an external contractor to manage computer or network facilities may introduce a number of potential security exposures, such as the possibility of compromise, damage, or loss of data at the contractor's site. These risks shall be identified in advance, and appropriate security measures agreed upon with the contactor and incorporated into the contract. Particular issues that shall be addressed are:
 - 1) Identification of any particularly sensitive or critical applications that would be better retained in-house;
 - 2) Approval of application guardians;
 - 3) Continuity plan implications;
 - 4) Security standards to be specified and process for measuring compliance;
 - 5) Responsibilities and procedures for reporting and handling security incidents;
 - 6) If the External Information System contains, or will contain Federal Tax Information (FTI), contact the Chief Information Security Officer before implementation to ensure applicable IRS guidelines are met.

B. Awareness and Training (AT)

Objective: To provide needed primary and ongoing security training for users of ODM IT resources. These policies and procedures reflect applicable state and federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1. AT-2 Security Awareness Training - ODM will provide basic security awareness training to all users, including contractors and non-ODM employees, covering applicable security threats within the organization.
 - a. Security Awareness Training - The Chief Information Security Officer and the Chief of Staff will ensure that each user, as part of the initial training for new users and annually thereafter, provide Security Awareness Training to all ODM users. This training will consist of practical exercises, which for example, may include attacks based on social engineering, email attachments, spear phishing attacks, malicious web links, and insider threats. Additional training may be required by information system changes and/or evolving threats. User's completion of this training will be recorded and maintained by the Chief of Staff and available for compliance reporting.

C. AT-3 Role Based Security Training

Objective: User Training is necessary to ensure that security procedures are correctly followed, and to minimize possible security risks to the confidentiality, integrity and availability of information or services due to user error.

1. New Employee On-Boarding - All users must receive appropriate training in organizational policies and procedures, including security requirements and other controls as well as training in the correct use of IT facilities (e.g., Building Access, Environmental Controls, logon procedure, use of software packages and changing passwords) before access to IT services is granted. The Office of Human Resources (HR) has the responsibility of documenting the on-boarding process and ensuring this training is completed and recorded.
2. Role Based User Training - All users must receive appropriate role based training for their specific role within the organization. This includes any security controls, policies, and procedures specific to their role. This training is also required before granting access to IT services impacted by the user's specific role(s). The respective program area is responsible for role based training documentation. The user's manager is responsible for assuring the user is training for their specific role(s), and that this training is recorded.
3. AT-4 Security Training Records
 - a. Training Record Documentation - ODM shall document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
 - b. Security Record Retention - ODM shall retain all individual security training records for seven calendar years.

D. Audit and Accountability (AU)

Objective: To provide audit trail generation, which assuring non-repudiation of the audit information, for the purposes of serving accountability, investigations, and reporting.

These policies and procedures reflect applicable state and federal laws, Executive Orders, directives, regulations, policies, standards and guidance.

1. AU-2 Audit Events

- a. Defining Audit Events -All audit events, for each information system or information system component, shall be defined in the Privacy Impact Assessment (PIA) document. The ITS Information Security Team will review each PIA, and provide guidance on the selection of appropriate audit events.

Examples of appropriate Audit Events:

- 1) Password Changes
- 2) User Creation, Deletion, or Lockout
- 3) Accessing, Modifying, or Deleting Confidential Personal Information (CPI).
- 4) Role Assignments for Role Assignment changes
- 5) Failed Logons
- 6) Failed Accesses related to information systems
- 7) Administrative privilege usage
- 8) Third-party credential usage
- 9) System Error events

2. AU-3 Content of Audit Records

- a. Minimum Audit Record Content - Each information system's audit record, when and where appropriate, possible, and applicable shall contain the following information:

- 1) what type of event occurred
- 2) when the event occurred,
- 3) where the event occurred,
- 4) the source of the event,
- 5) the outcome of the event,
- 6) And the identity of any individuals or subjects associated with the event.

3. AU-4 Audit Storage Capacity

- a. Audit Storage Considerations - Information system Owners much consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. The storage capacity allocated shall be monitored periodically to ensure that the allocation isn't exceeded, or so that data can be archived periodically for the storage capacity increased.

4. AU-5 Response to Audit Processing Failures

-
- a. Audit Processing Failure Handling - Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Each Information System must generate Audit Processing Failure alerts and send them to the appropriate personnel for resolution. The Information System must also define the appropriate action that occurs when Audit Processing fails. Audit Failure Responses can be:
 - 1) Shut down the Information System
 - 2) Overwrite the oldest audit records
 - 3) Stop generating audit recordsWhen assigning the appropriate action for the Audit processing failure, consideration must be given to applicable state and federal laws, codes, directive and regulations. Consult the Information Technology team to ensure your Audit processing failure response is in compliance with legal and regulatory requirements.
5. AU-6 Audit Review, Analysis, and Reporting
 - a. Periodic Review and Analysis of Audit Records - Each System Owner is responsible for generating Audit Reports, that detail all audit events captured within their sphere of responsibility, and reviewing them periodically. This review shall occur as often as applicable state and federal laws, Executive Orders, directives, regulations, policies, standards, and guidance dictate. Any detected security related incidents shall be communicated through Agency incident response procedures (See section VI, Policy (13) "Incident Response" section IR-4 and IR-6 within this document).
 - b. System Audit Requirements - Audit requirements and activities involving checks on operational systems shall be carefully planned to minimize the risk of disruptions to operating processes. The following shall be observed:
 - 1) Audit requirements shall be agreed upon between appropriate management.
 - 2) The scope of the checks shall be agreed upon and controlled.
 - 3) The checks shall be limited to read-only access to software and data.
 - 4) Other types of access (other than read-only) shall only be allowed for isolated copies of system files, which shall be erased when the audit is completed.
 - 5) IT resources for performing the checks shall be explicitly identified and made available.
 - 6) Requirements for special or additional processing shall be identified and agreed upon with service providers.
 - 7) All access shall be monitored and logged to produce a reference trail.
 - 8) All procedures, requirements and responsibilities shall be documented.
 6. AU-7 Audit Reduction and Report Generation
 - a. Audit Reduction and Reporting - Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. The summary information can then be used to generate on-demand reports for audit review and analysis to support after-the-fact investigations of security incidents. The Audit reduction must not alter the
-

original content or time ordering of the audit records. Each information System shall have the ability to do audit reduction and generate this information into a report.

7. AU-8 Time Stamps
 - a. Clock Synchronization - The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. ODM system device clocks shall be synchronized to approve Agency time sources and because some clocks are known to drift with time, there shall be a procedure that checks for and corrects any significant variation.
 - b. Audit Log Time Stamps - Each Audit Event time stamp must remain the same during Audit Generation, consolidation, Reduction and Reporting.
8. AU-9 Protection of Audit Information
 - a. Protection of System Audit Tools - Access to system audit tools, e.g., software or data files, shall be safeguarded to prevent any possible misuse or compromise. Such tools shall be separated from development and operational systems and not held in libraries or user areas unless given an appropriate level of additional security protection.
 - b. Restricted Subset of Users having Access to Audit Info - Individuals with privileged access to an information system and who are also the subject of an audit by that system may affect the reliability of audit information by inhibiting audit activities or modifying audit records. Therefore efforts shall be taken, within each information system, to restrict access of audit information to a subset of users who have privileged access, or another set of users who operate independently for the purpose of investigations.
9. AU-10 Non-repudiation
 - a. Non-repudiation protections - Each information system shall protect against an individual (or process acting on behalf of an individual) falsely denying having performed an action with an information system. Information System Auditing processes can ensure non -repudiation by:
 - 1) Protecting Audit Records from alteration, or access by unauthorized personnel.
 - 2) Utilizing digital signatures, or hashes to prove the validity of the audit record(s)
 - 3) Immediately and automatically sending all audit records to a secure centralized Audit logging server that has restricted, controlled access.
10. AU-11 Audit Record Retention
 - a. Audit Record Retention Length - Each Information System shall retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This length of time is varied for each

Information System, but it shall be based on applicable state and federal laws, Executive Orders, directives, regulations, policies, standards and guidance dictate. The Period of time shall be defined in the appropriate Privacy Impact Assessment (PIA) for the Information System, Application or Service.

11. AU-12 Audit Generation

- a. Report Generation - Each Information System shall be capable of generating reports for audit events defined in the Privacy Impact Assessment (PIA). This reporting function must also be able to do audit reduction, and report on all audit record contents.

E. Security Assessment and Authorization (CA)

Objective: To manage a risk-based Information Security program and provide a process for Certification and Accreditation for ODM information systems. These policies and procedures reflect applicable state and federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1. CA-2 Security Assessments - The ODM Chief Information Security Officer will ensure that Security Assessments will be conducted for ODM Information Systems by the Ohio Office of Budget and Management (OBM) - Office of Internal Audits (OIA). OIA will audit major information systems as a continuing engagement. The finding of these audits will be presented to ODM upon their conclusion.
2. CA-3 System Interconnects
 - a. Data and Software Exchange Agreements - Formal agreements shall be established for exchange of data and software (electronic and manual) between the Ohio Department of Medicaid and external organizations. The security content of such an agreement shall reflect the sensitivity of the information involved. Agreements shall specify appropriate security conditions including the following:
 - 1) Management responsibilities for controlling and notifying transmission and receipt;
 - 2) Procedures for notifying transmission and receipt;
 - 3) Minimum technical standards for packaging and transmission;
 - 4) Courier identification standards;
 - 5) Responsibilities and liabilities in the event of loss of data;
 - 6) Data and software guardianship and responsibilities for data protection, software copyright compliance and similar considerations;
 - 7) Technical standards for recording and reading data and software;
 - 8) Any special measures required to protect very sensitive items such as encryption keys.It is the responsibility of each Security Designee to document, establish and maintain these Data Sharing Agreements. Approval from the ODM Chief Privacy Officer is required for all Data Sharing Agreements.
3. CA-5 Plan of Action and Milestones

-
- a. Plan of Action and Milestone (PoAM) - System Developers, both internal and external, will develop a Plan of Action and Milestones (PoAM) document that will be updated and reported to Business Owners at least quarterly. The PoAM document will also include dates and timelines for each time. The Plan of Action and Milestones document will track Information System/Application:
 - 1) enhancements;
 - 2) coding flaw remediation;
 - 3) vulnerability remediation;
 - 4) security controls from the Corrective Action Plan(s) (CAP).

 4. CA-6 Security Authorizations
 - a. Information Security Certification & Accreditation Program - Federal law requires ODM to implement a risk-based program for cost-effective security on systems with their information. All business processes operate with some level of risk, and one of the most effective ways to protect these business processes is through the implementation of effective internal security controls, risk evaluation, and risk management.
 - b. Certification - The objective of the Certification phase is to determine through testing the extent to which the security controls in an information system are implemented as described, operating with minimal risk, and producing the desired outcome. The Business Owner certifies the information system for processing before operations and certification is updated at least every year. The Business Owner shall:
 - 1) Direct the System Developer to identify a sub-set of security controls to be tested with the objective to validate all of the security controls at least once every three years using standard testing procedure and techniques for the annual Security Test & Evaluation.
 - 2) Ensure the annual Security Test & Evaluation is conducted.
 - 3) Develop Corrective Action Plan(s) in collaboration with the System Developer when new vulnerabilities are identified and include them in the next quarterly Plan of Action and Milestone.The System Developer (either ITS Program Build Team for internal development or Contractors for external development) shall:
 - 1) Conduct the annual Security Test & Evaluation.
 - 2) Develop Corrective Action Plan(s) in collaboration with the Business Owner when new vulnerabilities are identified and include them in the next quarterly Plan of Action and Milestone.
 - c. Accreditation - The objective of the Accreditation phase is to determine whether the remaining known vulnerabilities in the information system pose an acceptable level of risk to ODM business, operations, and assets. The Chief Information Officer authorizes (i.e. accredits) the information system for processing before operations and the authorization (i.e. accreditation) is updated at least every three years.

The Business Owner shall:

 - 1) Assemble and deliver the Certification & Accreditation package to the Chief Information Security Officer containing at minimum:
-

- a) Updated Privacy Threshold Analysis (PTA) or Privacy Impact Assessment (PIA)
 - b) Updated System Security Plan.
 - c) Updated Information Security Risk Assessment.
 - d) Latest annual Security Test & Evaluation
 - e) Updated Plan of Action and Milestone.
- 2) Brief the Chief Information Officer and the Chief Information Security Officer on the information system, its business function, its security controls and the risk it imposes on ODM business, operations and assets.
 - 3) Modify, if necessary, the information system and/or the Certification & Accreditation package based on any action items from the briefing and/or accreditation corrective actions or restrictions.

The Chief Information Security Officer shall:

- 1) Review the residual risk to ODM business, operations, and assets based upon the confirmed vulnerabilities in the information system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities in the Certification & Accreditation package.
- 2) Determine if the residual risk to ODM business, operations, and assets is acceptable.
- 3) Provide any remaining accreditation corrective actions or restriction in the information system briefing to the Chief Information Officer.

The Chief Information Officer shall:

- 1) Review the Certification & Accreditation package and consider issues discussed at the information system briefing.
- 2) Make an accreditation decision:
 - a) a full accreditation,
 - b) a conditional authority to operate with terms and conditions for system operation, or denial to operate until required accreditation corrective actions are completed.
- 3) Sign the Accreditation Letter as Authority to Operate prior to the expiration of the previous accreditation (at least every three years). The Chief Information Officer may declare the operation of the system as unauthorized if the Business Owner does not obtain re-accreditation by the expiration of the previous accreditation.

5. CA-7 Continuous Monitoring

- a. Continuous Monitoring of Information Systems - Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms "continuous" and "ongoing" imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support Agency risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions (remediation or mitigation) by Guardians of Information Systems. Where possible, the assessment of the state of Vulnerability Management shall be assessed by independent assessors or using automated products that provide a

consistent, independent, uniform assessment. ODM has defined a continuous monitoring strategy, this strategy is to:

- 1) Conduct vulnerability scanning at least quarterly
- 2) Assign a priority to detected vulnerabilities
- 3) Track remediation and mitigating actions
- 4) Report vulnerability management conditions to executive staff for risk management decisions.

The ITS Program Run Team has responsibility for executing the continuous monitoring strategy.

6. CA-9 Internal System Connections

a. Documentation of Internal System Inter-Connections - Information systems across the Agency often utilize data/information or services from other internal information systems within its bounds of operation. This is common and to be expected, however these inter-connections must be authorized by the Business and System Owners of the Interconnecting Information System in writing. Additionally, the technical details of the inter connections shall be documented. At a minimum, this document will include the following information:

- 1) authorization for interconnect;
- 2) the interface characteristics;
- 3) security requirements;
- 4) controls to safeguard the information;
- 5) the nature of the information communicated.

This documentation shall be stored with the Project and System Documentation.

F. Configuration Management (CM)

Objective: To provide a uniform set of policies and procedures to measure compliance of Configuration Management items across the Agency. These policies and procedures reflect applicable state and federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1. CM-2 Baseline Configurations

a. Information System Baseline - Each System Owner shall document a baseline for the entire Information System; the Baseline shall include the following information:

- 1) Communication paths and connectivity-related detail, including data interconnects.
- 2) Hardware (including Firmware details) and Operating System information for each component.
- 3) Supporting Applications, Services, and Software detailing the name and version of each.
- 4) Technologies employed in the design and operation of the Information System.
- 5) Configuration Files

This Baseline shall be updated each time a change in the information system occurs related to the Baseline Information. All previous Baselines shall be retained for record keeping and rollback purposes. Production Baselines shall be stored separately from any Development or Test Environment Baselines. When Infrastructure for Information System isn't being hosted within internal Agency Datacenters, the third party hosting environment is required to supply any necessary information related to the documentation of the Baseline. This documentation shall be stored with all other appropriate Project and System documentation.

- b. High Risk Areas - When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. Contact CISO for advice when additional security controls are needed, and which security controls to employ in these scenarios.
 - c. Control of Operational Software - Strict control shall be exercised over the implementation of software on operational systems. The following controls shall be implemented to minimize the risk of corruption of operational systems:
 - 1) The updating of the operational program libraries shall only be performed by the nominated librarian upon authorization from the IT support manager for the application.
 - 2) If possible, only executable code shall be held on operational systems.
 - 3) Executable code shall not be implemented on an operational system until evidence of successful testing and user acceptance is obtained and the corresponding program source libraries have been updated.
 - 4) An audit log shall be maintained of all updates to operational program libraries.
 - 5) Previous versions of software shall be retained as a contingency measure.
 - 6) The Information System Baseline Documentation needs to be updated (See above CM-2 (A) "Information System Baseline")
2. CM-3 Configuration Change Control
 - a. Operational Change Control - Changes to IT facilities and systems shall be controlled. Inadequate control of changes to IT facilities and systems is a common cause of system or security failures. Therefore, formal management responsibilities and procedures are necessary to ensure satisfactory control of all changes to equipment, software or procedures. Appropriate change control procedures shall be documented in the IT Change Control Standards. ITS Configuration and Change Management Unit are responsible for documenting and maintaining these procedures.
 3. CM-4 Security Impact Analysis
 - a. Security Review of Changes to Information Systems - The ITS Information Security Team will be contacted to conduct a security impact analysis for all

changes to Information Systems for the Agency. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analysis may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. The review of these changes shall take place prior to the final design, and before major coding operations begin.

4. CM-5 Access Restriction for Change
 - a. Authorizations to perform Changes in Production - Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore only qualified and authorized individuals are allowed to access information systems for purposes of initiating changes, including upgrades and modifications. Each System Owner shall maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions shall organizations discover any unauthorized changes.

5. CM-6 Configuration Settings
 - a. Device Configuration Settings and Compliance - Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings care be defined include, for example:
 - 1) mainframe computers,
 - 2) servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name),
 - 3) workstations,
 - 4) input/output devices (e.g., scanners, copiers, and printers)
 - 5) network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors),
 - 6) operating systems, middleware , and applications.Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example:
 - 1) registry settings;
 - 2) account, file, directory permission settings;
 - 3) settings for functions, ports, protocols, services, and remote connections.Each System Owner will establish a defined set of configuration settings and parameters for categories of devices managed within their sphere of control. The System Owner will ensure the consistent enforcement of these configuration setting and parameters across all of their managed devices. Once a baseline of configuration settings and parameters are defined, all changes to the baseline shall then go through the Operation Change Control Process. The ITS Information Security Team will

- periodically review these configuration settings and parameters to ensure they are in compliance with state and federal laws, executive orders, directives, regulations, policies, standards, and guidance.
6. CM-7 Least Functionality
 - a. Restricting information systems to only essential functions - Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operation (e.g., key missions, functions). Additionally, it is sometime convenient to provide multiple services provided by any one component. Where feasible, information systems component functionality shall be limited to a single function per device (e.g., email servers or web servers, but not both). System Owners shall review functions and services provided by information systems or individual components of information system, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). System Owners shall disable unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. The ITS Information Security Team will periodically utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls, proxy servers, and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, applications, and services.
 7. CM-8 Information System Component Inventory
 - a. Information System Inventory
System Owners must develop an Information System Component Inventory, or utilize an Agency centralized inventory system, to develop and document an inventory or information system components that:
 - 1) Accurately reflects the current information systems;
 - 2) Includes all components within the authorization boundary of the information system;
 - 3) Is at a level of granularity necessary for tracking and reporting;
 - 4) Reviews and updates the information periodically as changes occur.
 8. CM-9 Configuration Management Plan
 - a. Change Control Procedures - In order to minimize the corruption of information systems, there shall be strict control over the implementation of changes. Therefore, formal change control procedures are necessary. They shall ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for them to perform their jobs, and that formal interdisciplinary agreement and approval for any change are obtained. This process shall include:
 - 1) Maintaining a record of agreed upon authorization levels including:

-
- a) IT support team focal point for change requests;
 - b) User authority for submission of change requests;
 - c) User authority levels for acceptance of detailed proposals;
 - d) User authority for the acceptance of completed changes;
 - 2) Only accepting changes submitted by authorized users;
 - 3) Reviewing security controls and integrity procedures to ensure that they will not be compromised by the changes;
 - 4) Identifying all computer software, data files, database entities and hardware that require amendment;
 - 5) Obtaining approval for detailed proposals before work commences;
 - 6) Ensuring that changes are accepted by the authorized user before implementation;
 - 7) Ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;
 - 8) Maintaining a version control for all software update;
 - 9) Maintaining an audit log of all change requests.
 - b. Technical Review of Operating System Changes - Periodically it is necessary to change the operating system (i.e. to install a new vendor-supplied release). When changes occur, the application systems shall be reviewed to ensure that there is no adverse impact on security. This process shall include:
 - 1) Review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;
 - 2) Ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;
 - 3) Ensuring that notification of operating system changes are provided in time to allow appropriate reviews to take place before implementation.
9. CM-10 Software Usage Restrictions
- a. Control of Proprietary Software Copying - Commercial software is protected by federal copyright and patent laws. Software publishers have organized under a group called the Software Publishers Association (SPA) to battle against infringement of copyright laws. The Ohio Department of Medicaid and associates are subject to audits by this group, and could face severe financial, civil, and criminal penalties for infringement of copyright laws. This policy ensures that ODM associates are aware that they need to adhere to software license agreements and protect the publisher's and author's right under these agreements. This policy applies to all software residing on computers, including games, screen savers, graphics and sound packages, text, binaries, graphics, etc. This policy applies to all ODM owned computers without regard to the location in which they are used (office, home, travel). All software residing on ODM computers must be licensed for use on the machine on which it resides. Associates and contractors will use, make and/or distribute copies of software only in accordance with the terms of the applicable license agreement. Software purchased for use on ODM computers will be tracked through ITS' Finance Unit. If software is acquired without the assistance of the Finance Unit, appropriate documentation must be

sent to the Finance Unit for purposes of license verification. The ITS Finance Unit will ensure that site licenses are properly maintained. The finance Unit is responsible for developing and maintaining software license maintenance procedures which meet or exceed those required by the Software Publishers Association. LAN software may be copied for backup and archival purposes, by the Finance Unit only. Beta programs and evaluation copies may be installed for a limited period of time as approved by ITS management for end user, network, and development applications.

10. CM-11 User-Installed Software

- a. User-Installed Software - Installation of unapproved software is prohibited by Agency users. IPP 10002 "Computer and Information Systems Usage" states: "All software installed on any ODM computer must be licensed to ODM. Personnel must receive advance approval from their deputy director and the Office of Information Technology Services (ITS) deputy director (or their respective designees) before adding software programs to any ODM computer. Questions regarding currently authorized software programs and/or software licensed to ODM are to be directed to the ITS deputy director or designee. "Reference IPP 10002 "Computer and Information Systems Usage" for the most current language of this policy statement.

G. Contingency Planning (CP)

Objective: To provide a uniform set of policies and procedures to ensure that continuity of services and availability of Information Systems across the Agency. These policies and procedures reflect applicable state and federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

NOTE: Contingency Planning issues are addressed at a high level in this document. Contact the appropriate department for additional information, as needed.

1. CP-2 Contingency Plan

- a. Developing a Business Continuity Plan - Each Information System needs to identify, as part of the system development life cycle, need to develop a needs to identify and develop a Business Continuity plan that:
 - 1) Identifies essential missions and business functions and associated contingency requirements;
 - 2) Provides recovery objectives, restoration priorities, and metrics;
 - 3) Addresses contingency roles, responsibilities, assigned individuals with contact information;
 - 4) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
 - 5) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;

-
- 6) Is reviewed and approved either during the Security Certification & Accreditation Program for major Information Systems, or during the Project Management phase by the Business and System Owners.
 - 7) It is the responsibility of ITS Change Control Review Board to ensure that adequate Contingency Plans are in place prior to Information Systems being released into production.
 - 8) Actions addressed in Business Continuity Plans include, for example, orderly/graceful degradation, information system shutdown, fallback to manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary Business Continuity planning activities are in place and activated in the event of a security incident.
- b. Resumption of Business Function timeframe - The Business Continuity Plan will define a timeframe for Business Resumption of each identified essential mission/business functions of the Information System. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure, and shall be reflected for each disruption scenario.
 - c. Fallback Planning - An emergency fallback facility provides an alternative, temporary means of continuing processing, in the event of any damage to, or failure of, equipment. Computer and network managers shall ensure that appropriate fallback arrangements are established for each IT service. Fallback requirements for individual systems shall be specified by the continuity planning process. Service providers shall coordinate fallback requirements for shared services and draw up an appropriate fallback plan for each service. Fallback facilities and procedures shall be regularly tested.
 - d. Capacity Planning - Capacity requirements shall be monitored to avoid failures due to inadequate capacity. Projections of future computer capacity requirements shall be made to ensure that adequate processing power and storage remain available. These projections shall take into account new system requirements as well as current and projected trends in computer and network use. Computer and network managers shall use this information to identify and avoid potential bottlenecks that might present a threat to system security or user services and plan appropriate remedial action.
 - e. Coordinate with Related Plans - Each Information System Continuity Plan must relate to, and be part of, the contingency plans for the agency. These plans include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation plan, and Occupant Emergency Plans.
 - f. Identify Critical Assets - Each Information System, as part of the Continuity Planning process, shall identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that

organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets.

2. CP-3 Contingency Training

- a. Role Based Training and Frequency - The Business owners will ensure that contingency training is provided to information system users consistent with assigned roles and responsibilities:

- 1) Within one month of assuming a contingency role or responsibility;
- 2) When required by information system changes;
- 3) At least annually thereafter.

Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential function in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflect the specific continuity requirements in the contingency plan.

3. CP-4 Contingency Plan Testing

- a. Contingency Plan Testing Requirements - Each Business and System Owner:
- 1) Tests the contingency plan for the information system at least annually to determine the effectiveness of the plan and the organizational readiness to execute the plan;
 - 2) Reviews the contingency plan test results;
 - 3) Initiates corrective actions, if needed.

Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. The Agency conducts testing based on the continuity requirements in contingency plans and includes a determination of the effects on organizational operations, assets, and individuals arising due to

contingency operations. The Agency has flexibility and discretion in the breadth, depth, and timelines of corrective actions.

4. CP-6 alternative Storage Site
 - a. Determining if an Alternative Storage Site is needed - Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of back up media. During Continuity Planning, if an Alternative Storage Site is needed based on requirements, the Alternate storage site needs to reflect the requirements identified in contingency planning so that the Agency can maintain essential missions/business function despite disruption, compromise, or failure in organizational information systems.
NOTE: Alternative Storage Sites for IRS Federal Tax Information (FTI) data. See IRS Publication 1075 for specifics on storing IRS FTI data at an Alternative Storage Site.
 - b. Alternative Storage Site Accessibility during an Area-Wide Disruption
Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., flood, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example:
 - 1) duplication backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or
 - 2) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.
5. CP-7 Alternative Processing Site
 - a. Designating and Alternative Processing Site - An Alternative Processing Site or Alternative Work Site is defined by the Chief Inspectors Office, and published and updated on the Agencies Intranet. This information is also distributed in the Agency-Wide Safety/Security Action Plan (ASAP). This Alternative Work Site will be separated geographically from the primary work site. The Alternative Work Site will have all the needed connectivity (data and voice) to perform their job function. It is the responsibility of the Employee's direct Manager to inform the employee of this information and his role, and need to report to the Alternative Work Site, in the event of an emergency requiring activation of the Alternative Work Site. Review of the ASAP safety and security procedures, and Alternative Work Site requirements, with a new or transfer employee must be performed within two weeks of their start date.
 - b. Priority-of-Service agreements - Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirement and the availability of information resources at the alternate processing site. Depending on the

Alternative Work Site Arrangements and business need, the Business owner, may need to negotiate such an agreement.

6. CP-9 Information System Backup
 - a. Backup Requirements - The System Owner shall:
 - 1) Conduct backups of user-level information contained in the information system
 - 2) Conduct backups of system-level information contained in the information system
 - 3) Conduct backups of information system documentation including security-related documentation; and
 - 4) Protect the confidentiality, integrity, and availability of backup information at storage locations.
 - 5) Periodically tests the backup information to verify the media's reliability and information integrity.

Backups will be conducted at a frequency and in a manner consistent with requirements defined in the continuity Plan for the timely resumption of essential missions/business functions.

7. CP-10 Information System Recovery and Reconstitution
 - a. Recovery and Reconstitution of the Information System - Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. Each Business and System Owner must define, in the Continuity Plan, all steps for the full reconstitution of the Information System to a fully operational state.
 - b. Transaction Recovery - Where possible, the information system shall implement transaction recovery for systems that are transaction-based. Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

H. Identification and Authentication (IA)

Objective: To provide a uniform set of policies and procedures for user and device identification and authentication for the Agency. These policies and procedures reflect

applicable state and federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1. IA-2 User Identification and Authorization
 - a. User Password Management - Passwords are currently and principal means of validating a user's authority to access a computer service. The allocation of passwords is controlled by a formal management process, which the Chief Information Security Officer controls, the requirements of which are as follows:
 - 1) Require users to sign a form indicating that they understand that they must keep personal passwords confidential.
 - 2) Where users are required to maintain their own passwords, they are provided initially with a temporary password which they are forced to change immediately.
 - 3) Temporary passwords are also provided when users forget a password, always subject to positive user identification. Temporary passwords are conveyed to users in a secure manner. Conveyance of passwords through third parties or through unprotected e-mail messages is prohibited.
 - 4) Users must acknowledge receipt of passwords, or access will expire after seven days. All departments administering passwords are required to follow this management process.
 - b. User Password Use - Users must follow appropriate security practices in the selection and use of passwords. Passwords are the principal means, at this time, of validating a user's authority to access a computer service. All users must adopt the following guidelines for managing their passwords:
 - 1) It is the responsibility of each user to safeguard his or her confidential password and to follow appropriate security practices in the selection and use of passwords.
 - 2) Select passwords with a minimum length of eight characters.
 - 3) Use passwords that cannot be easily guessed by others or through use of automated tools. If possible, include non-alpha characters in passwords. Do not use words that can be found in dictionaries of any language.
 - 4) Avoid passwords based on any of the following:
 - a) names (user, spouse, children, pets, etc.);
 - b) months of the year, days of the week, etc.;
 - c) social security numbers;
 - d) company name;
 - e) phone numbers;
 - f) user ID name;
 - g) more than two consecutive identical characters.
 - 5) Under no circumstances shall you share your password with anyone (in person or by telephone) regardless of who the person claims to be.
 - 6) Change passwords at least every 60 days, or at any time a user feels the password has been compromised.
 - 7) Do no reuse passwords for at least three generations.
 - 8) Change temporary passwords at the first logon.

-
- 9) Never embed a user-code and password in macros, scripts, job control language, or programs, unless they have been robustly encrypted.
 - 10) Do not allow others to observe the entering of passwords.
 - c. Password Management System - An effective password system must be used to authenticate users. Passwords are the principal means of validating a user's authority to access a computer service. Password management systems must provide an effective, interactive facility which ensures quality passwords. A good password management system shall:
 - 1) enforce the use of individual passwords to maintain accountability;
 - 2) allow users to select and change their own passwords and include a confirmation procedure to allow for typing errors;
 - 3) enforce a minimum length of eight characters for passwords;
 - 4) where users maintain their own passwords, enforce a password change at regular intervals (i.e., every 60 days);
 - 5) enforce a more frequent password change of every 30 days for privileged accounts (i.e., those with access to system utilities);
 - 6) where passwords are selected by the users, force them to change temporary passwords at the first logon;
 - 7) not display passwords on the screen when being entered;
 - 8) store password files separately from the main application system data;
 - 9) store passwords in encrypted form, using a one-way encryption algorithm;
 - 10) alter default vendor passwords following installation of software.
2. IA-3 Device Identification and Authorization
- a. Node Authentication - A facility for automatic connection by a remote computer could provide a means of unauthorized access to an application. Connections by remote computer systems shall therefore be authenticated. This is especially important if the connection is via an open network that is outside the control of ODM's security management. Authentication can be carried out at the application, computer or network level. An assessment of organizational risks and impacts may be required to determine the requirements for remote authentication. At the network level, authentication of a remote system can be achieved by node-authentication using, for example, a challenge/response system or a line encryption system. Dedicated private lines or a network user address (NUA) checking facility can also be used to provide assurance of the source of connections.
 - b. Unattended User Equipment - Users must ensure that unattended equipment has appropriate security protection. Equipment installed in user areas (e.g., workstations or file servers) may require specific protection from unauthorized access when left unattended for an extended period. All users and contractors must be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users shall adopt the following good practices:
 - 1) Terminate active sessions when finished, unless they can be secured by an appropriate lock.

-
- 2) Log off mainframe computers when the session is finished. Do not just switch off the PC or terminal.
 - 3) Log off or lock your screen when you leave your workstation.
 - 4) Log off, and restart your workstation when leaving at the end of the work day. The workstation will enter a low power sleep mode. ODM Office of Information Services (ITS) performs after hours patching, scanning, and maintenance on workstations, in order to increase user productivity ITS requires that users leave their workstation on overnight.
- c. Automatic Terminal Identification - Automatic terminal identification shall be considered to authenticate connections to specific location. Automatic terminal identification is a technique that can be used for applications in which it is important that the session can only be initiated from a particular location. An identifier in, or attached to, the terminal can be used to indicate which a particular terminal is permitted to initiate or receive certain transactions. It may be necessary to apply physical security protection to the terminal to maintain the security of the terminal identifier.
3. IA-4 Identifier Management
- a. User Identifiers - All users must have a unique identifier (user ID) and unique email address for their personal and sole use to ensure that activities can subsequently be traced to the responsible individual. User IDs shall not give any indication of the user's privilege level (e.g., manager, supervisor), or the application system to which they give access.
4. IA-5 Authenticator Management - Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length).
- a. Verifying the recipient of the Authenticator - Information Security Access Control, as part of the initial authenticator distribution, must define processes to identify the individual, group, role, or device receiving the authenticator. Where possible, the authenticator shall have a limited amount of reuse whether by time or by the number of uses.
 - b. Establishing Authenticator Procedures - Information Security Access control in conjunction with the Business and System Owners must define administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
 - c. Transmission of Authenticator information - The Information System must ensure the encrypted storage and transmission of Authenticator information (username, password, tokens, etc.) to protect the confidentiality and integrity of the Authentication process.
 - d. Default Authentication credentials - In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. Each
-

System Owner must change these default Authenticators to protect the Integrity of the Information System.

5. IA-6 Authenticator Feedback
 - a. Obscuring Authenticator Feedback - The Information System must ensure the feedback from authenticator input does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shaller surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for very limited time before fully obscuring it.

6. IA-8 Identification and Authentication of Non-Organizational Users
 - a. Non-Organizational Users - Non-organizational users include information system users other than organizational users explicitly covered by IA-2. The information system needs to uniquely identify and authenticate non-organizational users (or processed acting on behalf of non-organizational users). Additionally, any Privacy-related information of this user must be protected in a manner that meets the requirements of applicable federal, state and county laws, Executive Orders, directives, policies, regulations, standards, and guidance.

I. Incident Response (IR)

Objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents. These policies and procedures reflect applicable state and federal laws, Executive Orders, directives, regulation, policies, standards, and guidance.

1. IR-2 Incident Response Training
 - a. Communicating and Handling Incidents - It is the responsibility of each manager to ensure their direct report employee is trained on Agency procedures for Incident Response and Reporting.

2. IR-3 Incident Response Testing
 - a. Testing Incident Response - The Chief Information Security Officer will periodically perform tests, from either an internal or external resource, to ensure the accuracy and workflow of the Incident Response Procedures and related applications. This test will be conducted at least annually.

3. IR-4 Incident Handling

-
- a. Incident Management Procedures - Incident management responsibilities must be established to ensure a quick, effective and orderly response to security incidents. The following guidelines shall be followed in developing incident management procedures:
- 1) The procedures shall cover all potential types of security incidents including:
 - a) system failures and loss of service;
 - b) errors resulting from incomplete or inaccurate data;
 - c) breaches of confidentiality.
 - 2) In addition to normal contingency plans, the procedures shall cover:
 - a) analysis and identification of the cause of the incident;
 - b) planning and implementation of remedies to prevent recurrence;
 - c) collection of audit trails and similar evidence;
 - d) communication with users and others affected by, or involved with, recovery from the incident.
 - 3) Audit trails and similar evidence shall be collected and secured for:
 - a) internal problem analysis
 - b) use as evidence in relation to potential breach of contract or breach of regulatory requirement;
 - c) negotiating for compensation from software and service suppliers;
 - d) evidence in the event of proceedings under computer misuse legislation.
 - 4) Action to correct and recover from security breaches and system failures shall be carefully and formally controlled. The procedures shall ensure that:
 - a) only clearly identified and authorized staff are allowed access to live systems and data;
 - b) all emergency action is reported to management and reviewed in an orderly manner;
 - c) the integrity of systems and security controls is confirmed with minimal delay.
4. IR-6 Incident Reporting
- a. Reporting Security Incidents - Security incidents must be reported immediately by filing an incident report through the ODM Chief of Staff. The incident report is available online through the Medicaid Central:
<https://odmweb.odjfs.state.oh.us/Pages/IncidentReport.aspx>. Reports will be routed to the Chief Information Security Officer and other ITS staff as appropriate. The Chief of Staff will notify the Chief Privacy Officer immediately if the incident involves a breach of confidential information.
 - b. Reporting Security Weaknesses - Users of IT services must note and report any observed or suspected security weaknesses in, or threats to, systems or services. Users must report these matters either to their management or directly to the Chief Information Security Officer via the ITS Service Desk as soon as possible. Users shall not attempt to prove a suspected weakness, as this might be construed as a misuse of the system.
 - c. Reporting Software Malfunctions - Users of IT services shall report on any software that does not appear to be functioning correctly (i.e., according to
-

specification) to the ITS Service Desk. If it is suspected that the malfunction is due to a malicious piece of software (e.g., a computer virus), please complete the following steps:

- 1) Note the symptoms and any messages appearing on the screen.
 - 2) Stop using the computer and isolate it if possible.
 - 3) Inform the Chief Information Security Officer via the ITS Service Desk.
- Users shall not attempt to remove the suspected software. Recovery shall be carried out by appropriately trained and experienced staff. The Chief Information Security Officer or designee will coordinate the recovery with the ITS staff and others as appropriate. (See IPP 10004 "Incident Reporting")

J. Maintenance (MA)

Objective: To establish a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls. These policies and procedures reflect applicable state and federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1. MA-2 Controlled Maintenance

- a. Equipment Maintenance - IT equipment shall be correctly maintained to ensure its continued availability and integrity. The following shall be observed:
 - 1) Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications.
 - 2) Repairs and servicing of equipment shall only be carried out by authorized maintenance personnel.
 - 3) A record of all faults or suspected faults shall be kept.
- b. Maintenance - The objective of the Maintenance phase is to provide on-going oversight and monitoring of the security controls implemented specific to an information system.

The Business Owner shall:

- 1) Document the proposed changes to the information system.
- 2) Perform an Information Security Risk Assessment prior to implementing any significant changes to the system to determine the potential impact of the changes on the security of the system.
- 3) Direct the System Developer to identify a sub-set of security controls to be tested with the objective to validate all of the security controls at least once every three years using standard testing procedures and techniques.
- 4) Ensure the testing is conducted.
- 5) Develop Corrective Action Plan(s) in collaboration with the System Developer with new vulnerabilities are identified and include them in the next quarterly Plan of Action and Milestone.
- 6) Authorize all actual changes to the system.

- 7) Review the revised Information Security Risk Assessment and Corrective Action Plan(s). If the changes to the system is not significant and the risk level remains the same or lower;
 - a) Then the changes may proceed.
 - b) Else submit the Certification & Accreditation package to the Chief Information Officer for re-accreditation.

The System Developer shall:

- 1) Document the actual changes to the information system.
- 2) Conduct the testing.
- 3) Develop Corrective Action Plan(s) in collaboration with the Business Owner when new vulnerabilities are identified and include them in the next quarterly Plan of Action and Milestone.

2. MA-3 Maintenance Tool

- a. Use of System Utilities - Most computer installations have one or more maintenance or system utility programs that might be capable of overriding system and application controls. It is essential that the use of such utilities is restricted and tightly controlled. The following controls shall be applied, where possible:
 - 1) Password protection for utilities;
 - 2) Segregation of utilities from applications software;
 - 3) Limitation of the use of the utilities to the minimum practical number of trusted, authorized users;
 - 4) Authorization for other ad hoc use of utilities;
 - 5) Limitation of the availability of utilities (i.e., for the duration of an authorized change);
 - 6) Logging of all use of utilities;
 - 7) Defining and documenting authorization levels for utilities;
 - 8) Removal of all unnecessary utility and system software.

3. MA-4 Nonlocal Maintenance

- a. Remote Nonlocal Maintenance - All Nonlocal Maintenance, that is maintenance and diagnostic activities whose activities are conducted by individuals communicating through an external network (e.g., the Internet), are to be approved by the Chief Information Security Officer, prior to executing those maintenance activities. All Nonlocal Maintenance is to be logged, by the respective ITS staff performing or authorizing, the Nonlocal Maintenance. These logs must be maintained for at least one calendar year.
- b. Remote Diagnostic Port Protection - Access to diagnostic ports must be securely controlled. Many computers have dial-up remote diagnostic facilities for use by maintenance engineers. If unprotected, these diagnostic ports may provide a means of unauthorized access. They must therefore be protected by an appropriate security mechanism (i.e., a key lock and a procedure to ensure that they are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access).

4. MA-5 Maintenance Personnel
 - a. Authorized Maintenance Personnel - Each System Owner shall document a list of authorized individuals, both internal to the organization, escorted support personnel performing maintenance, and non-escorted support personnel performing maintenance on their responsible information systems, components, application, or devices. Additionally, the manager will document the required access and authorization s pertinent to each maintenance activity. With Information Systems containing Federal Tax Information (FTI), all non-internal support personnel performing maintenance, they System Owner must first contact Information Security to ensure IRS guidelines are adhered to for the proposed /scheduled maintenance.

5. MA-6 Timely Maintenance
 - a. Support Agreements - Each System Owner shall maintain any contracts or agreements necessary for the maintenance or support of the continued operation of their information system, related components or applications. The response time of these agreements must reflect the importance to the agency of the respective information system, component, or application of which the maintenance or support agreement is being entered into. A copy of these contract or agreements shall be kept with the Project/System Documentation. Additionally, this support information shall be clearly communicated to all appropriate support staff.

K. Media Protection (MP)

Objective: This Media protection policy addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, compliance, and procedures to facilitate the implementation of the media protection policy and associated media protection controls. The Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1. MP-2 Media Access - Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm.
 - a. Restricted Access to Confidential Personal Information (CPI)
System Owners shall restrict access to CPI data contained within media for each Information System. The internal Policy detailing these requirements is ODM IPP 3925 "Data Access Policy."
 - b. Restricted Access to Federal Tax Information (FTI) System Owners shall restrict access to FTI data contained within media for each Information System. This restriction shall be done in accordance with requirements set for in the most current version of the IRS Publication 1075 "Tax Information Security Guidelines for Federal, State, and Local Agencies."

-
2. MP-3 Media Marking
 - a. Management of Removable Computer Media - Each System Owner shall establish procedures for the management of removable computer media, such as tapes, disks, removable storage devices and printed reports and related required markings. The following controls shall be applied in the operational environment:
 - 1) If no longer require, erase the previous contents of any reusable media that are to be removed from the organization.
 - 2) Require a written authorization for all media removed from the organization and keep record of all such removals to maintain an audit trail.
 - 3) Store all media in a safe, secure environment in accordance with manufacturers' specifications.
 - 4) All procedures and authorization levels shall be clearly documented.
 - b. Federal Tax Information (FTI) Media Markings - System and Business Owners must ensure that Federal Tax Information (FTI) data media markings are in compliance with requirements set for in the most current version of the IRS Publication 1075 "Tax Information Security Guideline for Federal, State and Local Agencies."
 3. MP-4 Media Storage
 - a. Safeguarding of Organizational Records - Important records can be contained on both digital and non-digital media. Important records of an organization shall be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory requirements as well as to support essential organizational activities. It is appropriate to destroy records that have been retained beyond the statutory retention time, if this does not have an adverse impact on organization operations. To meet these obligations, the following steps shall be taken:
 - 1) Guideline shall be issued on the retention, storage, handling and disposal of records and information.
 - 2) A retention schedule shall be drawn up identifying essential record types and period of time for which they shall be retained.
 - 3) An inventory of sources of key information shall be maintained.
 - 4) Appropriate measures shall be implemented to protect essential records and information from loss, destruction and falsification.
 4. MP-5 Media Transport
 - a. Security of Media in Transit - Computer media can be vulnerable to unauthorized access, misuse or corruption during transportation. The following controls shall be applied to safeguard computer media being transported between sites:
 - 1) All portable media containing confidential information must be encrypted in a manner consistent with OIT encryption standards and must be FIPS 140-2 validated.
-

-
- 2) Reliable transport or couriers shall be used. A list of authorized couriers shall be agreed upon with management and a procedure to check the identification of couriers implemented.
 - 3) Packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.
 - 4) Special measures shall be adopted to protect sensitive information from unauthorized disclosure or modification. Examples include:
 - a) Use of locked containers;
 - b) Delivery by hand;
 - c) Securely sealed packaging which cannot easily come open while in transit.
 - d) Any exception to the above must be prior approved in writing by the ODM Chief Information Security Officer.
5. MP-6 Media Sanitation
- a. Secure deletion/Destruction of sensitive Information - An organization's information can be compromised through careless disposal of equipment. All items of equipment containing storage media (e.g., fixed hard disks shall be checked to ensure that any sensitive data and licensed software are removed or overwritten prior to disposal). Damaged storage devices containing very sensitive data may require a risk assessment to determine if the items shall be destroyed, repaired or discarded. Disposal of this media, within this equipment, shall be conducted in accordance with the latest revision of NIST Special Publication 800-88 "Guidelines for Media Sanitization."
 - b. Disposal of Media - Computer media shall be disposed of securely and safely when no longer required. Sensitive or restricted information may be leaked to outside persons through careless disposal of computer media. Clear procedures for the secure disposal of media shall be established to minimize this risk. The following guidelines shall be applied:
 - 1) Media containing sensitive or restricted information must be disposed of securely and safely (e.g., incineration) or emptied of data before use by another application within the organization.
 - 2) Use the following checklist to identify items that might require secure disposal:
 - a) input documents
 - b) carbon paper
 - c) output reports
 - d) one-time-use printer ribbons
 - e) magnetic tapes
 - f) removable disks
 - g) removable storage devices (e.g., flash drive)
 - h) program listings
 - i) test data
 - j) system documentation

-
- 3) Many organizations offer collection and disposal services for papers, equipment and media. Care shall be taken in selecting a suitable contractor with adequate security controls and experience.
 - 4) Disposal of restricted items shall be logged, when possible, for future reference and to maintain an audit trail. When accumulating information for disposal, consideration shall be given to the aggregation effect which may cause a large body of restricted information to become more sensitive than a small quantity of restricted information. Disposal of media shall be conducted in accordance with the latest revision of NIST Special Publication 800-88 "Guidelines for Media Sanitization."
6. MP-7 Media Use
- a. Security of Electronic Mail - Controls shall be applied to reduce the organizational and security risks associated with electronic mail (e-mail). E-mail is increasingly used for communications, replacing traditional forms of communication such as letters and faxes. E-mail differs from traditional forms of communication in its speed, message structure, degree of formality and vulnerability to interception. Consideration shall be given to the need for controls to reduce any organizational or security risks that may be presented by the introduction of e-mail. Issues that shall be addressed include the following:
 - 1) The vulnerability of messages to unauthorized interception or modification;
 - 2) The vulnerability to error (e.g., incorrect address or misdirection) and the general reliability and availability of the service;
 - 3) The impact of a change of communication media on organizational processes (i.e., effect of increased speed of dispatch or change from organization-to-organization to person-to-person addressing);
 - 4) Legal consideration such as the potential need for proof of origin, delivery and acceptance;
 - 5) The security implications of publishing directory entries;
 - 6) The need for security measures to control remote user access to e-mail accounts.
 - 7) Security of Electronic Office Systems (including Electronic Mail, Electronic Personal Calendars, etc.). Clear policies and guidelines are required to control the organizational and security risks associated with electronic office systems. Electronic office systems provide opportunities for faster dissemination and sharing of information. Each organizational unit shall consider the security and implications of such facilities, and the need for appropriate policies and guidelines. Requirements and issues which shall be addressed include the following:
 - a) the possible need to exclude any categories of sensitive or restricted information (e.g., classified information) if the system security does not provide an appropriate level of security protection;
 - b) the possible need to restrict access to diary information relating to selected individuals (i.e., staff working on sensitive projects);

- c) the suitability of the system to support applications, such as communicating orders or authorization;
 - d) the possible need to restrict selected facilities to specific category users;
 - e) the policy regarding retention and backup of information held on the system;
 - f) the requirements and arrangements for fallback.
- b. Data Handling Procedures - System Owners shall establish Procedures for handling sensitive and restricted data in order to protect such data from unauthorized disclosure or misuse. Procedures shall be developed for the secure handling of all sensitive and restricted input/output media, e.g., documents, tapes disks, reports and any other sensitive items (such as invoices). The following items shall be covered:
- 1) Handling and labeling input/output media;
 - 2) Maintenance of a formal record of the authorized recipients of data;
 - 3) Ensuring that input data are complete;
 - 4) Confirmation of receipt of transmitted media;
 - 5) Keeping the distribution of data at a minimum;
 - 6) Clear marking of all copies of data for the attention of the authorized recipient;
 - 7) Review of distribution lists and authorized recipient lists at regular intervals.

L. Physical and Environmental Protection (PE)

Objective: To develop procedures for the approval, and maintenance of a list of individuals with authorized access to the facility where the information system(s) reside, which also includes:

- a. Issuing authorization credentials for facility access;
 - b. Reviewing the access list detailing authorized facility access by individuals; and
 - c. Removes individuals from the facility access list when access is no longer required.
- The Chief of Staff is responsible for documenting these procedures.

NOTE: Physical security issues are addressed at a high level in this document. Contact the appropriate department for additional information, as needed.

- 1. PE-2 Physical Access Authorizations (See IPP 10200 "ODM Identification Badges")
- 2. PE-3 Physical Access Control - To prevent unauthorized access, damage and interference to IT services.
 - a. Physical Security Perimeter - Physical security protection shall be based on defined perimeters and achieved through a series of strategically located barriers throughout the organization. The requirements and setting of each security barriers shall depend upon the value of the assets and services to be protected, as well as the associated security risks and existing protective measures. Each level of physical protection shall have a defined security perimeter around which a consistent level of security protection is maintained. The Chief Information Security Officer shall be contacted, via the ITS Service Desk, for assistance in

developing plans for physical security of IT facilities. The following are guidelines:

- 1) The security of the perimeter shall be consistent with the value of the assets or services under protection.
 - 2) The security perimeter shall be clearly defined.
 - 3) Physical barriers shall, if necessary, be extended from floor to ceiling to prevent unauthorized entry and environmental contamination.
 - 4) Other personnel shall not be made aware unnecessarily of the activities within a secure area.
 - 5) Prohibition of individuals working alone shall be considered, both for safety and to prevent opportunities for malicious activities.
 - 6) Organizationally-managed computer equipment shall be housed in dedicated areas separate from third party-managed computer equipment.
 - 7) When vacated, secure areas shall be physically locked and periodically checked.
 - 8) Personnel supplying or maintaining support services shall be granted access to secure areas only when required and authorized. Where appropriate, their access shall be restricted (especially to sensitive information) and their activities monitored.
 - 9) Photography, recording or video equipment shall not be allowed, unless authorized with the security perimeters.
 - 10) Any Information System containing Federal Tax Information (FTI) shall be secured in accordance with IRS publication 1075. Contact the Chief Information Security Officer to ensure compliance with IRS guidelines.
 - 11) Any Information System containing Social Security Administration (SSA) data shall be secured in accordance with SSA requirements. Contact the Chief Information Security Officer to ensure compliance with SSA guidelines.
- b. Physical Entry Controls - Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. The following controls shall be considered:
- 1) Visitors to secure areas shall be supervised and their date and time of entry and departure recorded. Visitors shall only be granted access for specific, authorized purposes.
 - 2) All personnel shall be required to wear visible identification within the secure area and encouraged to challenge strangers.
 - 3) Access rights to secure areas shall be revoked immediately for staff who leave employment.
- c. Security of Data Centers and Computer Rooms - Data centers and computer rooms supporting critical organizational activities shall have effective physical security. The selection and design of the site shall take account of the possibility of damage from fire, flooding, explosions, civil unrest and other forms of natural or manmade disaster. Consideration shall also be given to any security threats presented by neighboring organizations and/or businesses. The following measures shall be considered:

- 1) Key facilities shall be sited away from areas of public access for direct approach by public vehicles.
 - 2) Where possible, buildings shall be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the present of computing activities.
 - 3) Lobby directories and internal telephone books shall not identify locations of computer facilities.
 - 4) Backup equipment and media shall be sited at a safe distance to avoid damage from a disaster at the main site.
 - 5) Appropriate safety equipment shall be installed, such as heat and smoke detectors, fire alarms, fire extinguishing equipment and fire escapes. Safety equipment shall be checked regularly in accordance with manufacturers' instructions. Employees shall be properly trained in the use of safety equipment.
 - 6) Emergency procedures shall be fully documented and regularly tested.
 - 7) Doors and windows shall be locked when unattended. External protection shall be considered for windows.
- d. Employee Desk Policy - In order to reduce the risks of unauthorized access, loss, and damage to information after normal working hours, sensitive and restricted papers and mobile storage devices that contains sensitive data shall not be left on desks unlocked. Information left out on desks is also likely to be damaged or destroyed in a disaster. The following guidelines shall be applied where appropriate:
- 1) Papers and mobile storage devices shall be stored in cabinets when not in use, especially outside of working hours.
 - 2) Sensitive or critical organizational information shall be locked away (ideally in a fire-resistant cabinet) when not required, especially when the office is vacated.
 - 3) Personal computers and computer terminals shall be protected by key locks, passwords or other controls when not in use.
 - 4) Consideration shall be given to the need to protect incoming and outgoing mail points and unattended fax machines.
 - 5) Laptops shall be secured by means of cable locks when in use at the desktop. Unattended laptops shall be secured by means of a cable lock or placed in a locked cabinet or drawer.
- e. Security of Equipment Off-Premises - IT equipment, regardless of guardianship, used outside the ODM premises to support organizational activities, is subject to management authorization and must be given the same degree of security protection as that of on-site IT equipment. The following guidelines must be applied:
- 1) When personal computers are used at home for business activities, virus controls must be in place.
 - 2) When traveling, equipment and media must not be left unattended in public places. Portable computers must be carried as hand luggage.

-
- 3) Portable computers are vulnerable to theft, loss or unauthorized access when traveling. They must be provided with an appropriate form of access protection (e.g., passwords or encryption) to prevent unauthorized access to their contents. The form of access control shall be based on the classification of the data stored on the machine.
 - 4) Manufacturers' instruction regarding the protection of equipment shall be observed at all times (i.e., to protect against exposure to strong electromagnetic fields). Security risks (e.g., damage, theft, eavesdropping) may vary considerably between locations and shall be taken into account in determining the most appropriate security measures. Contact the Chief Information Security Officer via the ITS Service Desk for assistance in determining the risk.
- f. Environmental Monitoring - Computer environments, including temperature, humidity and power supply quality, shall be monitored where necessary to identify conditions which might adversely affect the operation of computer equipment. These procedures shall be carried out in accordance with manufacturers' recommendations.
 - g. Prevention of Misuse of Facilities - The IT facilities of an organization are provided for organizational purposes. Their use shall be authorized by management. Any use of these facilities for non-organizational or unauthorized purposes without management approval and supporting accounting arrangements shall be regarded as improper use of the facilities. If such activity is identified by usage monitoring or other means, it shall be brought to the attention of the Chief Information Security Officer. Many countries have, or are in the process on introducing legislation to protect against computer misuse. It may be a criminal offense to use a computer for unauthorized purposes. It is essential therefore that all users are given written authorization of the precise scope of their permitted access. Employees of ODM and third party users shall be advised that no access is permitted except that which is formally authorized and documented.
 - h. Separation of Development and Operational Facilities - Development and testing activities may cause unintended changes to software and data that share the same computing environment. Therefore segregation of development and production operations activities is desirable to reduce the risk of accidental changes or unauthorized access to operational software and organizational data. The following internal controls must be adhered to, unless an exception is authorized by both the associated development Manager and ODM Chief Information Security Officer:
 - 1) Sensitive data must not be used for non-production purposes such as development, test and/or training unless irreversibly masked to make the sensitive data elements non-recognizable from their original content.
 - 2) Development and operational software shall run on different processors, domains, directories and/or logical partitions.
 - 3) Development and test activities shall be isolated from production operational environments and use of live data in these activities shall be limited to conversion testing and production break/fix situations.
-

-
- 4) Compilers, editors and other system utilities shall not be stored with operational systems, when not required.
3. PE-4 Access Control to Transmission Medium (See PE-9 for Cabling Security)
 4. PE-5 Access Control to Output Devices
 - a. Support functions and equipment (e.g., photocopiers and fax machines) shall be located to minimize the risks of unauthorized access to secure areas and sensitive information.
 5. PE-9 Power Equipment and Cabling
 - a. Cabling Security - Power and telecommunication cabling carrying data or supporting IT services shall be protected from interception or damage. The following security measures shall be applied to reduce these risks within an organization's premises:
 - 1) Power and telecommunications lines into IT facilities shall be underground or subject to adequate alternative protection.
 - 2) Measures shall be considered to protect network cabling from unauthorized interception or damage, for example, by using conduit or by avoiding routes through public areas.
 - 3) For exceptionally sensitive or critical systems, consideration shall be given to additional measures such as:
 - a) Use of data encryption;
 - b) Installation of armored conduit and locked rooms;
 - c) Use of alternative routing or transmission media.
 6. PE-16 Delivery and Removal
 - a. Isolated Delivery and Loading Areas - Computer rooms shall be protected from unauthorized access. An isolated area for delivery and loading of supplies and equipment is recommended in order to reduce the opportunity for unauthorized access to the computer room. The security requirements for such an area shall be determined by a risk assessment. The following guidelines shall be applied:
 - 1) Access to the holding area from outside the building shall be restricted to identified, authorized personnel.
 - 2) The holding area shall be designed so that supplies can be unloaded without gaining access to other parts of the building.
 - 3) The external door of the holding area shall be secured when the internal door is opened.
 - 4) Incoming material shall be inspected for potential hazards before it is moved from the holding area to the point of use.
 - b. Secure Disposal of Equipment - An organization's information can be compromised through careless disposal of equipment. All items of equipment containing storage media (e.g., fixed hard disks) shall be checked to ensure that any sensitive data and licensed software are removed or overwritten prior to
-

-
- disposal. Damaged storage devices containing very sensitive data may require a risk assessment to determine if the items shall be destroyed, repaired or discarded.
- c. Removal of Property - Equipment, data or software must not be taken off-site by employees without documented management authorization.
7. PE-17 Alternative Work Site
- a. The Chief of Staff's Office is responsible to designate, update, and communicate Alternative Work Sites for all authorized employees. This information is communicated through the "Agency Wide Safety/Security Action Plan" (ASAP) and given to an employee, during onboarding, by his or her supervisor where applicable by their position (required to report to alternative work site).
 - 1) Additionally, Alternative Work sites shall be used during Disaster Recovery Exercises to test Alternative Work site functionality.
8. PE-18 Location of Information System Components
- a. Locating information system components - Properly locating Information System Components to prevent loss, damage or compromise of assets, and interruption of organizational activities. IT equipment shall be placed or protected in a manner that reduces the risk of environmental hazards and opportunities for unauthorized access. The following guidelines shall be followed:
 - 1) Where possible, equipment shall be placed in secure locations in order to minimize unnecessary access into work areas. Workstations handling sensitive data shall be positioned in secure locations to reduce the risk of unauthorized access.
 - 2) The following checklist shall be used to identify potential hazards to IT equipment:
 - a) Fire
 - b) Smoke
 - c) Water
 - d) Dust
 - e) Vibration
 - f) Chemical effects
 - g) Electrical supply interference
 - h) electromagnetic radiation
 - 3) Consideration shall be given to potential hazards from neighboring floors as well as to those from the same floor.
 - 4) Eating shall be prohibited in computer equipment areas.
 - b. Power Supplies - Equipment shall be protected from power failures or other electrical anomalies. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications. Consideration shall be given to the possible need for a standby power supply. An uninterruptible power supply (UPS) is recommended for equipment supporting critical operations. Contingency plans shall cover the action to be taken after the UPS is exhausted. UPS equipment shall be regularly tested in accordance with the manufacturer's recommendations.
-

-
9. PE-20 Asset Monitoring and Tracking
 - a. Inventory of Assets - The departmental unit manager is responsible for maintaining an inventory of the major assets associated with each information system. Each asset must be clearly identified and its guardianship, retention schedule, and security classification agreed upon and documented. Examples of assets associated with information systems include the following:
 - 1) Information assets - databases and data files, system documentation, user manuals, training material , operational or support procedures, continuity plans, fallback arrangements;
 - 2) Software assets - application software, system software, development tools and utilities;
 - 3) Physical assets - computer and communication equipment, magnetic media, power supplies, air conditioning units;
 - 4) Services - computing, communications and facilities services required for operation.
 - b. Responsibility of Guardianship - The departmental unit manager must identify guardians for major assets and assign responsibility for the maintenance of appropriate security measures. Responsibility for implementing security measures may be delegated, but accountability will remain with the assigned guardian of the asset.

M. Planning (PL)

Objective: To ensure that adequate Information Security activities, initiatives, and requirements are integrated within Agency Strategic Planning and Information System Design. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1. PL-2 System Security Plan - The system developer, in conjunction with the system owner, business owner and the Chief Information Security Officer, will oversee the development of a security plan for each information system that:
 - a. Is consistent with the organization's enterprise architecture;
 - b. Explicitly defines the authorization boundary for the system;
 - c. Describes the operational context of the information system in terms of missions and business process;
 - d. Provides the security categorization of the information system including supporting rationale;
 - e. Describes the operational environment for the information system and relationships with or connections to other information systems;
 - f. Provides an overview of the security requirements for the systems;
 - g. Identifies any relevant overlays, if applicable;
 - h. Describes the security controls in place for planned for meeting those requirements includes a rationale for the tailoring and supplementation decisions;

-
- i. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; (See section CA-6 (A) for Information System Accreditation Process)
2. PL-4 Rules of Behavior - ODM shall establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; The user's manager manually or through automated means, requires and receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; Periodic revisions to these Rules of Behavior will require users who have signed previous versions of the Rule, to read and resign when the Rules of Behavior when revised/updated.
 - a. Personnel Expectations
 - 1) User Responsibilities - Users are responsible for making use of security measures to prohibit access to information on their workstations. Procedures and security alerts will be issued by both guardians and the Chief Information Security Officer. Users shall read these documents and contact the sender if they have any questions regarding the content. Users are also responsible for ensuring that unauthorized use of their assigned accounts is reported. Users are expected to review the date and time of previous successful logons when they log on to systems. If this information indicates that someone else has used they account, the Chief Information Security Officer or designee shall be contacted immediately via the ITS Service Desk. Prohibited activities include:
 - a) Crashing the system. It is noted that systems do crash, and that users may not recognize that they have been the cause of the crash. However, if the user's actions are traced as the cause of the crash and the user is notified as such, any repeat of the circumstances will be taken as a deliberate attempt to crash the system and will be dealt with accordingly.
 - b) Trying to defeat information system security. This includes running any password cracking programs, viruses, Trojan horses, sniffers, etc., as well as trying to circumvent file permissions on these systems and on systems connected via any network connection. Research into these types of activities is specifically prohibited, unless coordinated through the Chief Information Security Officer.
 - c) Creating any mail or network commands with false or anonymous origination information. This is in keeping with ODM policy of enforcing user accountability for all traffic on the system.
 - 2) Use of Organizational Resources - The ODM information computers and communications systems are the property of the Ohio Department of Medicaid and must be used for explicitly authorized purposes. To maintain and manage this property, ODM reserves the right to examine all data stored in, or transmitted by, these systems. Users of the Ohio Department of Medicaid computing services must not use these facilities for soliciting business, selling products, or otherwise engaging in commercial activities other than those

expressly permitted by ODM management. Electronic mail systems are intended to be used primarily for business purposes. Any personal use must not interfere with normal business activities; must not involve solicitation, must not be associated with any for-profit outside business activity; and must not potentially embarrass ODM. Users must not engage in inappropriate conduct such as use of electronic mail for unlawful or malicious activities; use of abusive or objectionable language in either public or private messages; misrepresentation of oneself or ODM; or other activities that could cause congestion and disruption of networks and systems, including the sending of chain letters. If there is a need to read another's ODM email (while they are away on vacation for instance), message forwarding/proxy services are required. Unauthorized copying (pirating) of copyrighted software is forbidden.

- 3) Privacy Expectations - ODM computer systems must be used for business purposes only and users have no expectation of privacy from ODM associated with the information they store in, or send through, these systems. Messages sent over the ODM electronic mail systems are not subject to the privacy provisions of the Electronic and Communications Privacy Act of 1986 (which prohibits wiretapping), and therefore may be read by management and system administrators.
 - 4) The Ohio Department of Medicaid Retains Ownership - All programs and documentation generated or provided by employees, consultants, or contractors for the benefit of ODM are the property of the Ohio Department of Medicaid unless other contractual arrangements are agreed upon and documented. Management must ensure that all workers developing programs or documentation sign a statement acknowledging ODM ownership prior to the provision of these materials.
- b. Internet Use Expectations
- 1) Acceptable Use - See IPP 10002 VI, B "Allowable Uses of Computers and Information Systems for ODM Business Purposes" & IPP 10002 VI, D, 3 c. "Internet Access Guidelines."
 - 2) Prohibited Activities - See IPP 10002 VI, C "Prohibited uses of Computers and Information Systems including, but not limited to, applications, e-mail, instant messenger (IM), short message service (SMS) text messaging, portable computing devices and the internet."
 - 3) Authorized Software - Only authorized software can be downloaded from non-ODM sources via the Internet and must be screened with virus detection software according to the current virus scan standard, prior to being invoked. All downloaded software shall be tested on a stand-alone non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine. The Chief Information Security Officer shall be notified of virus detection via the ITS Service Desk. All information taken off the Internet shall be considered suspect until confirmed by separate information from another source. There is no quality

control process on the Internet, and a considerable amount of information is outdated or inaccurate.

- 4) Confidential Personal Information (CPI) public disclosure ODM internal, sensitive and restricted information must not be sent over the Internet unless it has first been encrypted by approved methods. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet. Contact the Chief Information Security Officer for appropriate tools via the ITS Service Desk. Credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form. ODM associates using information systems and/or the Internet shall realize that their communications are not automatically protected from viewing by third parties.
 - 5) Establishing unapproved external connections - Unless prior approval from the Chief Information Security Officer has been obtained, associates and contracted employees may not establish Internet or other external network connections that could allow non-authorized users to gain access to systems and information. These connections include the establishment of multi-computer file systems (like Sun's NIS), Internet Home Pages, FTP servers and the like. Employees have an obligation to be aware of computer security and privacy concerns and to guard against computer viruses and security breaches of any kind. Any user who suspects that the network has been penetrated shall immediately contact the Chief Information Security Officer via the ITS Service Desk.
- c. Email Security
- 1) Outlook PST Files - PST files are permitted for usage on the ODM Network provided the following are adhered to:
 - a) All PST files are to be stored on a Network File Share only (Users personal drive), do not store PST files on your local workstation.
 - b) You must password protect your PST files so they are encrypted.
 - c) Your PST files do not leave the agency boundary
 - d) You must manage the size of your PST file to only keep messages that are required for the email retention period for the applicable line of business the mail is pertaining to.
 - 2) Emailing Federal Tax Information (FTI) - Employees are prohibited from sending Federal Tax Information using email. Exceptions to this policy must be granted by the ODM Chief Information Security Officer.
 - 3) Emailing Social Security Administration (SSA) Data- Employees are prohibited from sending SSA data via email. Exceptions to this policy must be granted by the ODM CISO.
- d. FAX Security
- 1) Faxing Federal Tax Information (FTI) - Employees are prohibited from sending Federal Tax Information using Fax machines or related Fax devices. Exceptions to this policy must be requested from the ODM Chief Information Security Officer.

-
- 2) Faxing Social Security Administration (SSA) Data- Employees are prohibited from sending SSA Data via fax or related devices. Exceptions to this policy must be requested from the ODM CISO.
3. PL-8 Information Security Architecture
 - a. Information System Alignment with Organizational Security Architecture
Information security architecture at the individual information system level needs to be consistent with and complement the more global, organization-wide information security architecture that is integral to and developed as part of the enterprise architecture.
 - b. Information Security Infrastructure
 - 1) Management Information Security Forum - Information security is an organizational responsibility shared by all members of the management team. The Chief Information Security Officer is responsible for leading the coordination of information security within the organization and will advise and seek the advice of the management team as necessary to:
 - a) Review and approve information security policy and overall responsibilities;
 - b) Monitor the exposure of major threats to information assets;
 - c) Review and monitor security incidents;
 - d) Approve major initiatives to enhance information security;
 - e) Perform other high-level information security management activities.
 - 2) Information Security Coordination - The Chief Information Security Officer and/or designees is responsible for coordinating the implementation of information security measures such as:
 - a) Establishing organization-wide Information Security Policy and Standards;
 - b) Monitoring and reporting effectiveness of system security and compliance with security policy;
 - c) Monitoring, investigating and resolving system security violations;
 - d) Assigning specific roles and responsibilities for information security across the organization;
 - e) Establishing methodologies and processes for information security, such as risk assessment and the security classification system.
 - f) Promoting the visibility of organizational support of information security throughout the organization;
 - g) Consulting with departmental units and information technology services groups on information asset security issues and techniques;
 - h) Ensuring that security is part of the information planning process;
 - i) Coordinating the implementation of specific information security measures for new systems or services;
 - j) Facilitating assignment of information asset guardianship;
 - k) Evaluating and recommending system security technology tools;
 - l) Approving guidelines and procedures developed under the Information Security Policy;

-
- m) Implementing access authorizations established by organizational units, as required.
 - 3) Security Designee - The departmental unit-appointed Security Designee are responsible for:
 - a) Assisting the Chief Information Security Officer in conveying information related to the protection of information assets and ensuring that the appropriate audience is reached;
 - b) Assisting IT and the Chief Information Security Officer in security incident response;
 - c) Participating in security awareness programs;
 - d) Ensuring that each system user is assigned an individual account and that the access requested is appropriate for the job responsibility (See IPP 3922 "Code of Responsibility" and IPP 3925 "ODM Data Access Policy");
 - e) Designating individuals who will be given authority to act in the Information Security Liaisons' absence and approve request for access upon completion of the Information Security Liaisons' awareness training;
 - f) Ensuring that the HIPAA Unit is immediately notified if an employee transfers to a new job function, is dismissed or resigned, so that system access can be appropriately deleted (see IPP 3927 "Computer System Access Termination");
 - g) Performing periodic reviews of user access to ensure that all accesses are appropriate and current (see IPP 3930 "Periodic Access Reconciliation").
 - 4) Allocation of Responsibilities - The security of an information system is the responsibility of the guardian of that system. Guardians of information systems may delegate their authority (power to act) to individual user managers or service providers. However, they remain ultimately accountable for protecting the security of the system. Therefore, the system guardian is responsible for ensuring that responsibilities are documented for each site, system and service to include:
 - a) Definition of the various assets and security processes associated with each individual system;
 - b) The manager assigned responsibility for each asset or security process;
 - c) Authorization levels assigned to each individual.
 - 5) Authorization Process for IT Facilities - A management approval process for new IT facilities (hardware, software, or network capabilities) is required to ensure that the installation of equipment is for a defined organizational purpose, will provide an adequate level of security protection, and will not adversely affect the security of the existing infrastructure. Two levels of approval are required:
 - a) Organizational approval - Each installation must have appropriate user management approval, authorizing its purpose and use. Approval must also be obtained from the manager responsible for maintaining the local information system's security environment, to ensure that it conforms to all relevant security policies and requirements.

-
- b) Technical approval - Each installation must have approval from IT and the Chief Information Security Officer to ensure that all devices connected to the ODM networks are of an approved device type and adequately secured.
 - 6) Specialist Information Security Advice - The ODM Chief Information Security Officer is the focal point for advice on implementing information security on all platforms.
 - 7) Independent Review of Information Security - The Information Security Policy (IPP 3001) sets out responsibilities and policy for the information security of the Ohio Department of Medicaid. The actual practice of information security will be reviewed periodically by the Chief Information Security Officer and/or Chief Legal Counsel and Chief of Staff to provide assurance that organizational practices properly reflect the policy.
4. PL-9 Central Management
- a. Compliance with Security Policy - All the Ohio Department of Medicaid departmental units are subject to review by the Chief Information Security Officer to ensure compliance with security policies and standards. Guardians of information systems must conduct regular reviews of the compliance of their systems with the appropriate security policies, standards and other security requirements.
 - b. Technical Compliance Checking - The Ohio Department of Medicaid Networks will be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to ensure that hardware and software security controls have been correctly implements. This monitoring will be performed by the Chief Information Security Officer or designee. Monitoring will be conducted using both manual and automated processes.

N. Program Management (PM)

Objective: To provide Organization-wide security context for all Information Systems within the Agency. These policies, procedures and Strategies reflect applicable state and federal laws, Executive Orders, directives, regulation, policies, standards, and guidance.

- 1. PM-2 Senior Information Security Officer
 - a. Chief Information Security Officer - The Agency's Chief Information Security Officer acts as the chief information security officer (CISO) for ODM.
- 2. PM-9 Risk Management Strategy - System owners, operators, and developers are required to adhere to an ongoing risk management strategy to safeguard systems and information.
 - a. Risk Management Framework (RMF)
 - b. Categorize - Complete FIPS 199 Categorization Worksheet (Reference RA-2 "Security Categorization")
 - 1) Do Impact Assessment (PIA) or Privacy Threshold Analysis (PTA).

-
- c. Select - Identify baseline controls upon category identified in step #1 using FIPS 200
 - 1) Refine - Use risk assessment to identify alternate compensating controls
 - 2) Document - Complete ODM System Security Plan (SSP) Based upon NIST families of controls
 - d. Implement - Prioritize implementation of security controls
 - 1) Leverage Council on CyberSecurity's "Critical Security Controls for Effective Cyber Defense (CSC)" to reduce risks
 - 2) Include any existing audit findings that would impact the system under evaluation
 - e. Assess
 - 1) Determine effectiveness of controls via:
 - a) automated vulnerability assessment tools,
 - b) Internal, state, and federal audit engagements
 - 2) Report monthly to the CIO, CISO, and other senior management
 - a) Vulnerability Assessment Reports
 - b) Audit POAMs/CAPs Status reports
 - f. Authorize - Complete ODM Certification and Accreditation form as part of System Security Plan (SSP)
 - 1) Accreditation
 - a) Program Deputy Director (Business Owner) signs to accredit the Information System for use within ODM.
 - 2) Certification
 - a) CIO signs to attest to security posture of application
 - g. Monitor
 - 1) Document any major system changes via ODM PIA
 - 2) Document all architectural changes within Enterprise Tools and Information System Documentation.
 - 3) Review SSP every 3 years
 - 4) Prepare risk assessment once every 3 years
 - 5) Leverage annual general controls audits
3. PM-18 Security authorization Process
- a. IRS 45 Day notification - All Major changes, to any information system containing Federal Tax Information (FTI), is required to provide the IRS notification 45 calendar days in advance of the change. This notification shall be conducted in accordance with requirements outlined in the most current revisions of IRS Publication 1075.

O. Personnel Security (PS)

Objective: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control that detail Agency requirements for individual positions and the employees within those positions. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1. PS-2 Position Risk Description
 - a. Security in Job Descriptions - Security roles and responsibilities shall be included in job descriptions where appropriate. Job descriptions shall include general responsibilities for implementing or maintaining security policy, as well as specific responsibilities for the protection of particular assets, or the execution of particular security processes or activities.
2. PS-3 Personnel Screening
 - a. Recruitment Screening - Applications for employment, whether permanent or temporary, must be screened if the job involves access to IT facilities that handle sensitive information. The following checks shall be made on all such applications: at least two satisfactory character references, one business and one personal; a check for completeness and accuracy of the applicant's resume; confirmation of academic and professional qualifications; and identification check (e.g., passport or birth certificate).
3. PS-4 Personnel Termination
 - a. Unit Responsible for handling Access Controls Tasks - The HIPAA Unit is responsible for establishing procedures for handling when an employee separates employment, and transfers/changes roles with the Agency.
 - b. Security Designees Roles - Security Designees and Information Security Liaisons are responsible for ensuring that the HIPAA Unit is immediately notified if an employee transfers to a new job function, is dismissed or resigns, so that system access can be appropriately deleted. (See IPP 3927 "Computer System Access Termination")
4. PS-5 Personnel Transfers (See PS-4 Personnel Termination)
5. PS-6 Access Agreements - Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the organizational information systems to which access is authorized.
 - a. Confidentiality Agreement - Users of the ODM IT facilities must sign an appropriate confidentiality or non-disclosure agreement. Employees shall sign such an agreement as part of their initial conditions of employment (see IPP 3922 and the 7078 code of Responsibility form).
6. PS-7 Third-Party Personnel Security Objection: To maintain the security of the ODM facilities and information assets accessed by third parties.
 - a. Identification of Risks from Third Party Connections - The security of the ODM systems might be put at risk from third party locations with inadequate security management. When there is a need to connect to a third party location, a risk analysis shall be conducted to identify any requirements for security measures.

The risk analysis shall take into account the type of access required, the value of the information, the security measures employed by the third party, and the implications of the access for the security of the ODM infrastructure. The Chief Information Security Officer, IT management, and/or the Legal department shall be contacted to assist in this process.

Access to the ODM Network shall not be provided to third parties until the appropriate measures have been implemented and a contract has been signed defining the terms for the connection

- b. Security Conditions in Third Party Contracts - Arrangements involving third party access to the ODM facilities shall be based on a formal contract containing all of the necessary security conditions to ensure compliance with the ODM security policies and standards. The contract shall be in place before providing access to IT facilities. The following items shall be considered for inclusion in the contract:
 - 1) Applicable sections of the ODM Information Security Policy (IPP 3001);
 - 2) Permitted access methods, and the control and use of unique identifiers (user IDs) and passwords.
 - 3) A description of each IT service to be made available;
 - 4) A requirement to maintain a list of individuals authorized to use the service;
 - 5) Times and dates when the service is to be available;
 - 6) The respective liabilities of the parties to the agreement;
 - 7) Procedures regarding protection of the assets, including information;
 - 8) Responsibilities regarding legal matters (e.g., data protection legislation);
 - 9) The right to monitor and revoke user activity;
 - 10) Responsibilities regarding hardware and software installation and maintenance;
 - 11) The right to audit contractual responsibilities;
 - 12) Restrictions on copying and disclosing information;
 - 13) Measures to ensure that return or destruction of information and assets at the end of the contract;
 - 14) Any required physical protection measures;
 - 15) Mechanisms to ensure that security measures are followed;
 - 16) User training in methods, procedures and security;
 - 17) Measures to ensure protection against the spread of computer viruses;
 - 18) An authorization process for user access;
 - 19) Arrangements for reporting and investigating security incidents;
 - 20) Acceptable involvement of third party subcontractors and other participants.
 - 21) Required adherence to ODM's code of responsibility (See IPP 3922 "Code of Responsibility")
 - 22) Required Internal Revenue Service Federal Tax Information Safeguard language (available from IRS Publication 1075 – "Tax Information Security Guidelines For Federal, State and Local Agencies.")
7. PS-8 Personnel Sanctions
 - a. Disciplinary Process - Failure to comply with the policies set forth in this document shall result in disciplinary action up to and including removal in

accordance with current disciplinary guidelines (see IPP 3922 and Disciplinary Grid).

P. Risk Assessment (RA)

Objective: The following security controls dictate how the Agency identifies, Classifies, Remediates, and Mitigates Information Security Risk. The following policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

1. RA-2 Security Categorization

- a. Information Classification - Security classification must be used to indicate the need and priorities for security protection.
- b. Classification Guidelines - Security classifications and associated protective measures shall be based on the organizational need for sharing or restricting access to the information, and the potential organizational impact associated with unauthorized access or damage to the information. The organizational need for confidentiality, integrity and availability of the information shall drive the classification. The assigned guardian is responsible for defining the classification of each item or information such as documents, data records, data files, or portable media, and for periodically reviewing the classification for continued appropriateness.
- c. ODM Security Classification Scheme - Each Information Type and Information System (consisting of one or many information types) must be documented, and follow the Security Categorization guidelines found in the Federal Information Processing Standards (FIPS) Publication 199 "Standards for Security Categorization of Federal Information And Information Systems." This Security Categorization can be contained in the project documentation or in the Information System Security Plan (SSP).

2. RA-3 Risk Assessment

- a. Assessing Security Risks - The expenditure on security controls needs to be balanced against the organizational value of the information. The Chief Information Security Officer will conduct periodic risk assessments, both internally and externally, to address the changing organizational priorities and threats to information. These risk assessments involve systematic consideration of the following:
 - 1) The nature of the information and systems;
 - 2) The business purpose for which the information is used;
 - 3) The environment in which the system is used and operated;
 - 4) The protection provided by the security controls in place;
 - 5) The organizational vulnerabilities that will likely result from a significant breach of security, taking into account possible consequences of failures of information confidentiality, integrity and availability;
 - 6) The realistic likelihood of such a breach occurring in the light of prevailing threats and controls.

The results of the risk assessment will determine appropriate priorities and action to take in implementing information security controls. A risk assessment can identify exceptional security risks which might require stronger controls than are stated in this policy. (See ODM Risk Management Framework (RMF) in PM-9)

3. RA-5 Vulnerability Scanning and Management
 - a. Vulnerability Scanning - The Chief Information Security Officer will direct the vulnerability scanning, detection, categorization, and reporting of vulnerabilities across the ODM Network.
 - b. Prioritization by Risk - The Chief Information Security Officer will direct the efforts for vulnerability remediation by assigning, by either manual or automated means, a prioritization of Vulnerabilities by Risk factors identified to the Agency.
 - c. Responsibility of Mitigation - The ITS Program Run Unit is responsible for mitigating and establishing exceptions based on operational requirements in a timely manner in accordance with the risk associated with the reported Vulnerability.

Q. System and Services Acquisition (SA)

Objective: To ensure that Information Security requirements are incorporated into the Agency's Information Systems for both developed and acquired/purchased systems.

NOTE: System and Services Acquisitions are addressed at a high level in this document. Contact the appropriate department for additional Policies and Procedures, as needed.

1. SA-2 Allocation of Resources
 - a. Information Security requirements incorporated into business planning The Chief Information Security Officer shall ensure that all information security requirements are incorporated into the Agency's mission and business plans. This includes the allocation of resources and funds required to protect information systems in the Agency's capital planning, budgeting, and investment Control Processes.
2. SA-3 System Development Life Cycle
 - a. Access Control to Program Source Library - In order to minimize the corruption of computer programs, strict control must be maintained over access to program source libraries for the entire System Development Life Cycle. When possible, source code management systems shall be utilized. The requirements for Source Control (also known as Version Control) control are as follows:
 - 1) Where possible, program source libraries shall not be held in operational systems.
 - 2) Roles and responsibilities need to be defined and documented for each user accessing the program source libraries. Additionally, a program librarian shall be nominated for each application.
 - 3) IT support staff shall not have unrestricted access to program source libraries.
 - 4) Programs under development or maintenance shall not be held in operational program source libraries.

-
- 5) The updating of program source libraries and the issuing of program sources to programmers shall only be performed by the nominated librarian upon authorization from the IT support manager for the application.
 - 6) Program listings shall be held in a secure environment.
 - 7) An audit log must be maintained of all accesses to program source libraries.
 - 8) Old versions of source programs must be archived with a clear indication of the precise dates and time when they were operational, together with all supporting software, job control, data definitions and procedures.
 - 9) Maintenance and copying of program source libraries are subject to strict change control procedure.
- b. Adherence to Security Engineering Principles during Design/Coding Qualified personnel, for example, Chief Information Security Officer, or security architects must be included in the system development life cycle activities to ensure that security requirements are incorporated into Agency information systems.
3. SA-4 Acquisition Process
 - a. System Acquisition Contracts- Requests for proposals and enacted acquisition contracts for new or updated information systems, system components, or information system services must include the following:
 - 1) Security Functional Requirements;
 - 2) Security Strength Requirements;
 - 3) Security Assurance Requirements;
 - 4) Security-related Documentation Requirements;
 - 5) Requirements for protecting security-related documentation;
 - 6) Description of the information system development environment in which the system is intended to operate;
 - 7) Acceptance criteria.
 - b. Design/Implementation Information for Security Controls - Contracted developers of information systems, system components, and/or information system services shall provide design and implementation information for the security controls which includes:
 - 1) Security-relevant external system interfaces
 - 2) High-level design;
 - 3) Low-level design;
 - 4) Source code or hardware schematics.
4. SA-5 Information System Documentation
 - a. Documented Operating Procedures - Documented operating procedures must be prepared for all operational computer systems to ensure their correct, secure operation. Documented procedures must also be prepared for systems development, maintenance or testing activities, and must recognize the support or attention expected of other organizational functions (e.g., computer operations). The procedures shall specify the correct instructions for the detailed execution of each job, including the following items, as appropriate:
 - 1) The correct handling of data files;

-
- 2) Scheduling requirements, including interdependencies with other systems, and earliest job start and latest job completion times;
 - 3) Instructions for handling errors or other exceptional conditions which might arise during job execution, including restrictions on the use of system utilities;
 - 4) Support contacts in the event of unexpected operational or technical difficulties;
 - 5) Special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs;
 - 6) System restart and recovery procedures for use in the event of system failure. Documented procedures shall also be prepared for system housekeeping activities associated with computer and network management, such as computer start-up and close-down procedures data backup, equipment maintenance, computer room management and safety. Operating procedures shall be treated as formal documents, changes to which shall only be made after approval by authorized management.
5. SA-8 Security Engineering Principles
- a. Security Requirements Analysis and Specification - An analysis of security requirement shall be carried out at the requirements analysis stage of each development project. Statements of requirements for new systems or enhancements to existing system shall specify the requirements for security controls. Such specifications normally focus on the automated controls to be incorporated in the system, but the need for supporting manual controls shall also be considered. These considerations shall also be applied when evaluating software packages for applications. Security requirements and controls shall reflect the value of the information assets involved and the potential damage which might result from a failure or absence of security. Two useful frameworks for guiding the analysis of security requirements are:
 - 1) Consideration of the need to safeguard the confidentiality, integrity and availability of information assets;
 - 2) Identification of the opportunities to use different types of controls to prevent, detect and recover from major failures or incidents. In particular, the analysis shall consider the need to:
 - a) control access to information and services, including any requirements for segregation of facilities or duties;
 - b) produce audit trails of important events for routine control or special investigation purposes, including evidence in contractual or other negotiations;
 - c) verify and protect the integrity of vital data in all or selected stages of processing;
 - d) protect confidential data from unauthorized disclosure, including the possible use of data encryption in special circumstances;
 - e) comply with regulatory, legislative or contractual requirement, including production of special reports to meet certain legislative requirements;

- f) take backup copies of essential data;
- g) recover from failures, especially for systems with high availability requirements;
- h) protect the system from unauthorized amendment or modification;
- i) enable the system to be operated and used securely by non-specialist (but suitably trained) employees;

Security controls incorporated in computer systems could be compromised if the IT support team and the users are not aware of them. Therefore, security controls shall be explicitly defined in all relevant documentation.

- 6. SA-11 Developer Security Testing and Evaluation
 - a. Protection of System Test Data - Test data shall be protected and controlled. System and acceptance testing usually require substantial amounts of test data that are as close as possible to the live data. The use of live databases containing personal data shall be avoided. If such data are used, they shall be depersonalized before use. The following controls shall be applied to protect live data when used for testing purposes:
 - 1) The access control procedures which apply to operational applications system shall also apply to test application systems.
 - 2) There shall be separate authorization each time live data are copied to a test application system.
 - 3) Live data shall be erased from a test application system immediately after the testing is complete.
 - 4) The copying of live data shall be logged to provide an audit trail.

R. System and Communication Protection (SC)

Objective: To protect all networked services and the communications that occurs across them. These policies and procedures reflect applicable state and federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

- 1. SC-2 Application Participation (Isolation)
 - a. Limited Services - The network and computer services that can be accessed by an individual user or from a particular terminal shall be consistent with the organizational access control policy. In particular, users shall only be provided with direct access to the services that they have been specifically authorized to use.
 - b. Enforced Path - The route from the user terminal to the computer service may need to be controlled. Modern networks are designed to allow maximum scope for sharing of resources and flexibility of routing. These features may also provide opportunities for unauthorized access to organizational applications or unauthorized use of the Ohio Department of Medicaid networks. These risks can be reduced by incorporating controls to restrict the route between a user terminal and the computer services that the user is authorized to access (i.e., creating an enforced path). The objective of such an enforced path is to prevent any undesirable straying by users outside the route between the user terminal and the

services that the user is authorized to access. This usually requires the implementation of a number of controls at several points in the route. The principle is to limit the routing options at each point in the network through predefined choices. Examples of this are as follows:

- 1) allocating dedicated lines or telephone numbers;
- 2) automatically connecting ports to specified application systems or security gateways;
- 3) limiting menu and submenu options for individual users;
- 4) preventing unlimited network roaming.

The requirements for an enforced path shall be based on the access control policy.

2. SC-3 Security Function Isolation

- a. Segregation in Networks - Large networks may need to be divided into separate domains. Computer networks are increasingly being extended beyond traditional organizational boundaries, as partnerships are formed that may require the interconnection or sharing of computer or network facilities. Such extensions might increase the risk of unauthorized access to existing computer systems that use the network, some of which might require protection from other network users because of their sensitivity or criticality. In such circumstances, the introduction of controls within the network, to segregate groups of users and computers, shall be considered.
 - 1) One method of controlling the security of large networks is to divide them into separate logical domain, each protected by the defined security perimeter, or firewall, and a network gateway. Access between domains can then be controlled by secure gateways, incorporating appropriate routing and connection-capability controls.
 - 2) The criteria for segregation of networks into domains is based on access control policy and requirements, and must also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.
- b. Limited Services - The network and computer services that can be accessed by an individual user or from a particular terminal shall be consistent with the organizational access control policy. In particular, users shall only be provided with direct access to the services that they have been specifically authorized to use.
- c. Enforced Path - The route from the user terminal to the computer service may need to be controlled. Modern networks are designed to allow maximum scope for sharing of resources and flexibility of routing. These features may also provide opportunities for unauthorized access to organizational applications or unauthorized use of the Ohio Department of Medicaid networks. These risks can be reduced by incorporating controls to restrict the route between a user terminal and the computer services that the user is authorized to access (i.e., creating an enforced path). The objective of such an enforced path is to prevent any undesirable straying by users outside the route between the user terminal and the services that the user is authorized to access. This usually requires the

implementation of a number of controls at several points in the route. The principle is to limit the routing options at each point in the network through predefined choices. Examples of this are as follows:

- 1) allocating dedicated lines or telephone numbers;
- 2) automatically connecting ports to specified application systems or security gateways;
- 3) limiting menu and submenu options for individual users;
- 4) preventing unlimited network roaming.

The requirements for an enforced path shall be based on the access control policy.

- d. Sensitive System Isolation - Sensitive systems might require a dedicated (isolated) computing environment. Some application systems are sufficiently sensitive to potential loss that they require special handling. The sensitivity may indicate that the application system shall run on a dedicated computer, only share resources with trusted applications systems, or have a no limitations. The following considerations apply:

- 1) The sensitivity of an application system shall be explicitly identified and documented by the application guardian;
- 2) When a sensitive application is run in a shared environment the application systems with which it will share resources shall be identified and agreed upon with the guardian of the sensitive application.

3. SC-4 Information in Shared Resources

- a. Preventing authorized or unattended information transfers - Each Information System must prevent information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address:

- 1) information permanence which refers to residual representation of data that has been nominally erased or removed;
- 2) covert channels (including storage and/or time channels) where shared resources are manipulated to violate information flow restrictions; or
- 3) components within information systems for which there are only singles users/roles.

4. SC-5 Denial of Service Protection

- a. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Protection
The ITS Program Run Team shall implement the following protections to limit DoS and DDoS attacks:

- 1) Implement DoS packet protection policies on boundary protection devices.
- 2) Ensure adequate bandwidth, and service redundancy is available.

-
- 3) Employ monitoring and detection tools to alert when indicator of DoS for DDoS is occurring against an information system or device.
 - 4) Restrict internal user's ability to launch a DoS or DDoS, either maliciously or unintentionally through a compromised host.
5. SC-7 Boundary Protection
- a. Network Connection Control - In order to support the access policy requirements of certain organizational applications, shared networks, especially those extending across organizational boundaries, may require the incorporation of controls to restrict the connection capability of the users. Such controls can be implemented through network gateways that filter traffic by means of predefined tables or rules. The restrictions applied are based on the access policy and requirements of the applications. Examples of such restrictions are:
 - 1) electronic mail only;
 - 2) one-way file transfer;
 - 3) two-way file transfer;
 - 4) interactive access;
 - 5) network access linked to time of day or date.
 - b. Network Routing Control - Shared networks, especially those extending across organizational boundaries, may require the incorporation of routing controls to ensure that computer connections and information flows do not breach the access policy of the applications. Routing controls are based on positive source and destination address checking mechanisms. They can be implemented in software or hardware. Implementers shall be aware of the strength of any mechanism deployed.
 - c. Security of Network Services - A wide range of public or private network services is available, some of which offer value-added services. These services may have unique security characteristics. Information Security must approve all external connections prior to implementation.
 - d. Separating Internal from External Networks - Sub-networks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.
 - e. The ITS Program Run Team has the responsibility of deploying technologies and network devices to provide this separation.
6. SC-8 Transmission Confidentiality and Integrity
- a. Protecting the Transmission of Data - Each information System must protect both the internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copier, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the

confidentiality and/or integrity of organizational information can be accomplished by:

- 1) physical means (e.g., employing physical distribution systems) or by
- 2) logical means (e.g., employing encryption techniques).

Information Systems relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situation, Business Owners must determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, they must implement appropriate compensating security controls utilizing Cryptographic Protection (see SC-13 Cryptographic Protection).

7. SC-10 Network Disconnect

- a. Session Termination and Timeout - Each information system must terminate the network connection associated with a user's communication session at the end of the session or after thirty minutes (or less) of inactivity. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions using a single, operating system-level network connection.
- b. Session Reuse - Once a Session is terminated either by the user or through an inactivity timeout, the session information must not be reusable at any point in the future.

8. SC-12 Cryptographic Key Establishment and Management

- a. Establishing and Managing Cryptographic Materials (Keys, Certificates, Passcodes) Managing Cryptographic materials is as important as the actual encryption operations themselves. If the Cryptographic Materials used to perform the encryption are compromised in addition to the encrypted data stream, it must be assumed that the entire communication is compromised and the related incident must be reported as such using Incident Reporting Procedures. Additionally, if the Cryptographic Materials are lost, the Agency may be unable to decrypt the information for restoration or investigation purposes. As a result, each Guardian of Information System(s) must:
 - 1) Establish Cryptographic key management processes or procedures using either manual procedures or automated mechanisms to protect this Cryptographic Material.
 - 2) Never store Cryptographic Materials used for encryption on the same server where the encryption is being performed.
 - 3) Protect Cryptographic Materials using encryption is required, if this information is stored on a Network Share or Database.

-
- 4) Where possible, establish Trust Stores (Enterprise Key and Certificate Management) to centralized and uniformly control, protect, and administer the Cryptographic Materials.
9. SC-13 Cryptographic Protection
 - a. Data Encryption - Encryption is the process of transforming information into an unintelligible form to safeguard its confidentiality and integrity during transmission or in storage. The process uses an encryption algorithm, secret key information, and message hashes or digital signatures, known only to the authorized users, to 'decrypt', use, and verify the integrity of the received information. Encryption must be employed in Information Systems containing Confidential Personal Information (CPI), Social Security Administration (SSA) data, or Federal Tax Information (FTI) data. Encryption for these information systems must be present in all three states of data, namely:
 - 1) Data in Motion
 - 2) Data at Rest
 - 3) Data in UseThe Encryption Modules used for this encryption must be approved, and be in accordance with State and Federal laws and regulations. Information Security shall be consulted to identify suitable products or modules that meet these requirements, and to ensure the security, retention, and handling of the related cryptographic materials (passcodes, keys, certificates, etc.). State of Ohio IT Standard ITS-SEC-01, 'Data Encryption and Cryptography,' requires cryptographic modules embedded in security services validated under the Cryptographic Module Validation Program (CMVP) in accordance with NIST FIPS Publication 140-2 be employed. Cryptographic module validation must be evidenced by a NIST-issued certificate number.
 10. Message Authentication – Message authentication, also known as a hash or digital signature, is a technique used to detect unauthorized changes to, or corruption of, the contents of a transmitted electronic message. It can be implemented in hardware, or software, using a physical message authentication device or a software algorithm. Message authentication shall be employed for applications where it is vital to protect the integrity of the message content (i.e., electronic funds transfers or other electronic data exchanges). An assessment of security risks, performed by Information Security, shall be carried out during the SDLC process to determine if message authentication is required and to identify the most appropriate method of implementation. Message authentication is not designed to protect the confidentiality of the data. Data encryption algorithms are the appropriate security control for this purpose.
 11. SC-17 Public Key Infrastructure Certificates
 - a. External Certificate Issuance - All Information Systems that have services available on the Internet that use Encryption (e.g., HTTPS), must use approved Public Key Infrastructure (PKI) Certificates so at the certificates are to be recognized as valid by common Intermediate and Root Certificates chains. See ITS Program Run Unit for the list of approved PKI providers.
-

-
12. SC-19 Voice over Internet Protocol (VOIP)
 - a. VOIP segmentation - If VOIP is used within the boundaries of an Information System the Business and System Owners must establish usage restrictions and implementation guidance for Voice over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and as such shall:
 - 1) Authorize the use of VOIP within the information system as part of the SSP and/or PIA.
 - 2) Monitor and Control the use of VOIP within the bounds of the Information System.
 - 3) Segment the VOIP network from the Information System Data Network.
 - a) Where possible, implement Firewalls and Boundary Protection between these Networks.
 - 4) Perform periodic security testing to ensure the established security controls are adequate to prevent damage.

 13. SC-21 Secure Name/Address Resolution
 - a. DNS Cache Poisoning Protection - The ITS Program Run Team shall implement necessary configuration and boundary defenses to ensure the integrity and data origin of Authoritative Name Resolution (e.g., Domain Name Service - DNS) Services both in resolving and in cached validation.
 - b. FQDN website access - When accessing internal and external websites, users shall use the fully Qualified Domain Name (FQDN). This is best practice and ensures that the proper site is being returned to the user (limiting phishing attacks) and that any predefined security certificates, based on the FQDN, can function as designed.

 14. SC-23 Session Authenticity
 - a. Preventing Man-in-Middle Attacks - Communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services), establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. This Authenticity protection includes, for example, protecting against man-in-the-middles attacks/session hijacking and the insertion of false information into sessions. Encryption and Digital Signatures are often used to ensure authenticity. The security controls implemented to meet this control must be defined and documented as part of the SDLC process, and in the System Security Plan (SSP) as applicable.

 15. SC-28 Protecting Data as Rest
 - a. Protecting the Confidentiality and Integrity of Information at Rest - Information at rest refers to the state of information when it is located on storage devices (e.g., Storage Array, Hard Disk, USB Drive, CD/DVD) as a specific component of an information system. Only sensitive information (CPI, PHI, PII, SSA, FTI data) needs to be protected at rest. Additionally, the confidentiality and integrity of all
-

backups of this sensitive information must be ensured. Encryption is the most common way to protect both the confidentiality and integrity of this Information. However, other valid methods and mitigating actions can be taken. The security controls implemented to meet this control must be defined and documented as part of the SDLC process, and in the System Security Plan (SSP) as applicable.

16. SC-39 Process Isolation

- a. Process Isolation - Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.

S. System and Information Integrity (SI)

Objective: To protect the integrity of operations of each Information System and the overall Agency. The following Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards and guidance

1. SI-2 Flaw Remediation

- a. Flaw Detection, Remediation, and Mitigation - ITS shall scan for Flaws in Information System components at least quarterly, using automated or manual tools. ITS shall organize these detected flaws, again using automated or manual means, to prioritize the list based on the highest risk factors to the Agency. This flaw information report will then be sent to the appropriate unit for remediation or mitigation. These unit's managers may also elect to accept the risk of the flaw in writing in lieu of performing remediation or mitigation actions based on business and operational requirements. ITS Program Run Management will establish timelines for remediation or mitigation based on the associated level of risk for the flaw.
- b. Agency Risk Tracking - Overall Agency Risk information will be communicated at least quarterly to ITS Senior Management for strategic planning and direction for Agency risk reduction.

2. SI-3 malicious Code Protection

- a. Malware Code Protection - Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code

protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In coordination with the Chief Information Security Officer, Guardians of Information Systems and the ITS Program Run Unit are responsible for implementing malware detection and prevention measures that:

- 1) Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
 - 2) Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
 - 3) Configures malicious code protection mechanisms to:
 - a) Perform periodic scans of the information system and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and
 - b) Block malicious code; quarantine malicious code; send alerts to administrators; in response to a malicious code detection; and
 - c) Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
3. SI-4 Information System Monitoring
- a. Monitoring Information Systems - The Guardians of Information System shall establish adequate monitoring tools and procedures to detect:
 - 1) Attacks and indicators of potential attacks, and
 - 2) Unauthorized local, network, and remote connections;
 - 3) Identify unauthorized use of the Information System
 - b. Intrusion-monitoring Information Systems (and for the organization) where applicable, deploy monitoring devices:
 - 1) strategically within the information system to collect organization-determined essential information; and
 - 2) at ad hoc locations within the system to track specific types of transactions of interest to the organization;The information obtained from intrusion-monitoring tools must be protected from unauthorized access, modification, and deletion.
 - c. Increased level of monitoring based on Risk to the Agency - Each Information System needs to be able to heighten the level of information system monitoring activity whenever there is an indication of increased risk to agency operations, assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

-
4. SI-5 Security Alerts, Advisories, and Directives
 - a. Response to Alerts, Advisories, and Directives = The Chief Information Security Officer shall have responsibility to oversee the receiving and the dissemination of security alerts, and advisories from the United States Computer Emergency Readiness Team (US-CERT), and directives, both State and Federal, for the Agency on an ongoing basis. Additionally, the CISO will ensure all directives are implemented within the established time frames for compliance, or notify the issuing organization of the degree of non-compliance.

 5. SI-8 Spam Protection
 - a. Limiting exposure to Spam email - ITS Program Run shall employ centralized tool(s) in partnership with OIT to limit the amount of Spam/Junk mail that enters the Agency. These tools can be employed to use automated or manual means of quarantine for these messages. Additionally, the tool(s) must allow for updates to spam protection mechanisms when new releases are available. ITS Program Run is responsible for defining agency procedures for Spam protection, and handling.

 6. SI-10 Information Input Validation
 - a. Input Data Validation - Data input to application systems shall be validated to ensure that it is correct and appropriate. The following controls shall be considered:
 - 1) Checks to detect the following error:
 - a) out-of-range values;
 - b) invalid characters in data fields;
 - c) missing or incomplete data;
 - d) exceeding upper and lower data volume limits;
 - e) unauthorized or inconsistent control data;
 - 2) Periodic review of the content of key fields or data files to confirm their validity and integrity;
 - 3) Inspecting hard-copy input documents for any unauthorized changes to input data (all changes to input documents shall be authorized);
 - 4) Procedures for responding to validation errors;
 - 5) Defining the responsibilities of all personnel involved in the data input process.
 - b. Internal Processing Validation - Data correctly entered into an application system can be corrupted by processing errors or through deliberate acts. Validation checks shall be incorporated into systems to detect such corruption. The specific controls required will depend on the nature of the application and the organizational impact of any corruption of data. Examples of checks that can be incorporated include the following:
 - 1) session or batch controls, to reconcile data file balances after transaction updates;
 - 2) balancing controls to check opening balances against previous closing balances, namely:
 - a) run-to-run controls;

-
- b) file update totals;
 - 3) program-to-program totals;
 - 4) validation of system-generated data;
 - 5) checks on the integrity of data or software downloaded or uploaded between central remote computers;
 - 6) hash totals of records and files.
7. SI-11 Error Handling
- a. Error Message Content - Each Information System needs to carefully consider the structure/content of error messages. The extent to which information system are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. As such, and Information System must:
 - 1) Generate error messages that provide information necessary for corrective action without revealing information that could be exploited by adversaries;
 - 2) Reveal error message only to appropriate administration staff.
8. SI-12 Information Handling and Retention
- a. Defining Information Handling and Retention requirements - Each Information System must define its Information Handling and Retention requirements within the Privacy Impact Assessment (PIA). The length of time for retention, and the nature of where it is retained from the Information System must be in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The ODM Privacy Officer is official keeper of PIA documents.
9. SI-16 Memory Protection
- a. Protecting Memory from unauthorized code execution - Some adversaries launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Systems shall deploy hardware-enforced or software-enforced with hardware data execution prevention safeguards to protect memory from unauthorized code execution.

VI. CONTACT:

Please direct all questions or concerns to IPP_ODM_Policy_Admin@medicaid.ohio.gov.

This Policy supersedes any previously issued directive or policy and will remain effective until cancelled or superseded.

VII. APPENDIX:

A. APPENDIX A: IT GLOSSARY

VIII. REVISION HISTORY:

Date	Description of Change
	Original

The ODM mission cannot be achieved without access to the Confidential Personal Information with which our clients and business partners have entrusted us. It is in the interest of maintaining and ensuring this trust that this policy seeks to establish the valid reasons for accessing these key information assets. The computer systems used in the delivery of services are large and complex in nature, as are the back-end data repositories that drive these systems. This makes for an extremely large array of confidential information that we are responsible for maintaining and protecting within these systems. Without this data, we could not function as an organization. Thus, anything that represents a threat to the security of this data, represents a threat to ODM ability to provide services. For this reason each employee must understand their vested interest in maintaining the security and privacy of the confidential information with which we have been entrusted. The purpose of the following is to provide clear guidance as to what is deemed valid access to ODM CPI and the legal basis for this guidance.

A. Criteria for accessing confidential personal information

1. The statutory definition of "CPI" is any personal information that is not considered public record under ORC 149.43. For ODM, CPI includes any non-public information about ODM employees, contractors and service providers (such as social security numbers and non-work-related addresses), as well as any information identifying applicants for, recipients of, and participants in Medicaid and other types of medical assistance.
2. ODM personal information systems are managed on a need to know basis, whereby each information owner determines the level of access required for an employee of the agency to fulfill his or her job duties. The determination of access to CPI must be approved by the employee's supervisor and the information owner prior to providing the employee with access to CPI within a personal information system. ODM has procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties, including but not limited to a transfer or termination. Whenever an employee's job duties no longer requires access to confidential personal information in a personal information system, then that employee's access to CPI shall be removed.

B. VALID REASONS FOR ACCESSING CPI

In general, any access to and use of CPI that is collected and maintained by ODM is strictly limited to those purposes authorized by ODM, and as directly related to the system user's official job duties and work assignments for, and on behalf of, ODM and/or a federal oversight agency. Some examples of when accessing CPI is prohibited include, but are not limited to, access that results in personal or political gain, and commercial use unrelated to official departmental business. Below is a list of valid reasons for accessing CPI (regardless of whether the CPI is maintained electronically or on paper).

1. In the course of administering or performing job duties related to the following processes, authorized employees of the agency would have valid reasons for accessing CPI:
 - a. Responding to (a) public records requests, when public records are comingled with CPI, or (b) records requests made by the individual for his/her own CPI;
 - b. Program administration, including (a) compliance with federal/state laws and regulations, (b) processing or payment of claims, (c) eligibility determinations (d) audits, investigations and oversight, (e) licensing and certification, and (f) administrative hearings;
 - c. Litigation (including discovery and responding to court orders and subpoenas);
 - d. Human resource matters (e.g. hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);
 - e. Complying with an Executive Order or policy;
 - f. Complying with an agency policy or a state administrative policy issued by the Department of Administrative Services, the Office of Budget and Management or other similar state agency;
 - g. Research in the furtherance of agency specific programs in so far as allowed by statute; or
 - h. Complying with a collective bargaining agreement provision.
2. In addition to the general processes described in paragraph (A) above, ODM must comply with numerous federal and state laws and regulations that limit its use and disclosure of CPI, including but not limited to:
 - a. 45 CFR Parts 160 and 164 (HIPAA-45 CFR 164.501);
 - b. 42 CFR 431.300 through 431.307 (Medicaid);
 - c. 5 USC 552a (Social Security Data);
 - d. Ohio Revised Code (ORC) sections:
 - (1) 5101.27 through 5101.31],
 - (2) 5101.99 (penalties for disclosure)
3. Intentional violations of this policy shall result in disciplinary action up to and including removal in accordance with current disciplinary guidelines.

VI. PROCEDURES:

- A. Any upgrades to existing ODM computer systems, or the acquisition of any new computer systems, that stores, manages, or contains Confidential Personal Information (CPI), shall include a mechanism for recording specific access by users of the system to CPI contained within that system. A systems upgrade is defined as any update requiring over half of the lines of code to be modified.
- B. Until an upgrade or new acquisition of the type described above occurs, each Office within ODM is responsible for documenting a manual logging procedure

for their staff. This procedure must be documented and forwarded for review to the ODM Chief Privacy Officer. Upon receipt of the documentation, the ODM Chief Privacy Officer will call upon the ODM Chief of Staff and Chief Legal Counsel or designees to perform a joint review of the manual logging process to validate that it will meet the requirements as set forth in the legislation. This document must show that the process captures the following fields:

1. Employee User Name
2. Date of Access
3. Time of Access
4. Name of Individual (First and Last) whose CPI was access
5. Name of computer system used to access CPI.

C. There exist two exceptions for the need to log access to CPI:

1. The access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals. e.g., a helpdesk staff person is requested to assist in the resolution of a program or technical issue, and in the course of resolving the issue, they must access CPI.
2. The access is to confidential personal information about an individual, and the access occurs as a result of a request by that individual or their legal representative for confidential personal information about that same individual

D. Information Requests

Upon the signed written request of any individual whose confidential personal information may be kept by the agency, the agency shall do all of the following:

1. Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information.
2. Provide to the individual the confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of chapter 1347 of the Revised Code.
3. During the pendency of an ongoing investigation about the individual, determine what, if any, records can be shared with that individual.

E. Notification of Invalid Access

1. Upon discovery or notification that CPI of a person has been accessed by an agency employee for an invalid reason, the agency shall take steps to notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. The agency shall delay notification for a period of time necessary to ensure that the notification will not delay or impede an

investigation or jeopardize homeland or national security. The agency may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information invalidly was accessed and to restore the reasonable integrity of the system. "Investigation" as used in this paragraph includes the investigation of the circumstances and involvement of employees surrounding the invalid access of the confidential personal information. Once the agency determines that notification will not delay or impede an investigation, the agency must disclose the access to confidential personal information made for an invalid reason to the subject of the CPI.

2. The notification given by the agency shall inform the person of the type of confidential personal information invalidly accessed and the date(s) of the invalid access (or as closely approximated as possible).
 3. Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.
- F. The ODM director shall designate an employee of the agency to serve as the Data Privacy Point of Contact under the working title of ODM Chief Privacy Officer. The Data Privacy Point of Contact shall work closely with the State of Ohio Chief Privacy Officer, the State Chief Information Security Officer, and the ODM Chief Information Security Officer to assist the agency with both the implementation of privacy protections for the Confidential Personal Information that the agency maintains and compliance with Section 1347.15 of the Revised Code and the rules adopted thereunder.
- G. The ODM Chief Privacy Officer will ensure the timely completion of the Privacy Impact Assessment form developed by the Office of Information Technology.
- H. The Privacy Impact Assessment will be used as a factor to define the security categorization of the information system in the System Security Plan.
- I. The guardian of the information system containing CPI will ensure the system uses encryption and authentication methods commensurate with requirements identified in the Privacy Impact Assessment and documented in the System Security Plan so as to ensure access to CPI is kept secured.
- J. All ODM employees must take part in a departmental training program that will at a minimum include awareness of all applicable statutes, rules, and policies governing access to confidential personal information with which they may come into contact as part of their assigned job duties.

-
- K. ODM will create a poster describing agency policies related to the protection of confidential personal information and post it in a conspicuous place in the main office of the agency and in all locations where the state agency has branch offices.
 - L. Receipt of this policy must be acknowledged by all agency employees.

VII. CONTACT:

Please direct all questions or concerns to IPP_ODM_Policy_Admin@medicaid.ohio.gov.

This Policy supersedes any previously issued directive or policy and will remain effective until cancelled or superseded.

VIII. APPENDIX:

A. IT GLOSSARY

IX. REVISION HISTORY:

Date	Description of Change
	Original

(Current as of August 26, 2015)

- A. **ACCESS:** to copy, view or otherwise perceive. As a verb, "access" means to copy, view or otherwise perceive.
- B. **ACQUISITION OF A NEW COMPUTER SYSTEM:** the purchase of a computer system, as defined in this chapter, which is not a computer system currently in place nor one for which the acquisition process has been started as of the effective date of the agency rule addressing ORC 1347.15 requirements.
- C. **ANONYMOUS FILE TRANSFER PROTOCOL (FTP):** Mechanism for downloading files from a website for which the user does not have an official password. The user cannot send (upload) files to the system or get access to its non-public sections.
- D. **AUTHORITATIVE SOURCE:** An ODM employee(s) with responsibility to authorize access for an external entity user(s), identify the level of access required, submit a formal request on behalf of the external entity user(s), and provide notice of access termination to ODM System Access Management.
- E. **AVAILABILITY:** Ensuring that information is available to users when required.
- F. **BUSINESS OWNER:** The designated ODM Program group that is responsible for the request, operation, and administration of an information system that supports its line of business.
- G. **CHIEF INFORMATION OFFICER (CIO):** The responsible Executive, who manages all Information Technology (IT) operations for the Agency.
- H. **CHIEF INFORMATION SECURITY OFFICER (CISO):** Responsible for coordinating the implementation of information security measures, and will assist the Legal and Audit departments in providing management assurance that departmental units are in compliance with policy, legislative and contractual requirements regarding information security.
- I. **CHIEF PRIVACY OFFICER:** The ODM designee charged with serving as the agency Data Privacy Point of Contact in accordance with ORC 1347.15(B)(7) charged to work with the State Chief Privacy Officer within the DAS Office of Information Technology to ensure that confidential personal information is properly protected.
- J. **COMPUTER SYSTEM:** a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains or retrieves personal information using electronic data processing equipment.
- K. **CONFIDENTIALITY:** Protecting sensitive information from unauthorized disclosure or interception.

- L. CONFIDENTIAL PERSONAL INFORMATION (CPI): As described in ORC 1347.15 (A)(1), CPI is personal information that is not a public record for purposes of section 149.43 of the Revised Code.
- M. CURRENT APPROVED SOFTWARE LIST: ITS will maintain and publish a list of software products that have been tested and verified for use on ODM network and for compatibility with other existing software.
- N. DIGITAL SIGNATURE: a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity).
- O. EMPLOYEE OF THE STATE AGENCY: employee of a state agency regardless of whether he or she holds an elected or appointed office or position within the state agency. "Employee of the state agency" is limited to the specific state agency that has the appointing authority for the employee.
- P. ENCRYPTION: Performed by hardware/software devices using a series of mathematical operations to scrambling sensitive information so that it becomes unreadable to everyone except the intended recipient.
- Q. EXTERNAL ENTITY: any non-ODM entity requesting access to an ODM controlled system or application. It includes business associates, county users, other state and federal agencies.
- R. FEDERAL TAX INFORMATION (FTI): As described in 26 USC Section(*) 6103 of the Internal Revenue Code, it is "Tax payer return and return Information". This information is to be kept confidential is subject to Safeguard requirements outlined in IRS Publication 1075 "Tax Information Security Guidelines for Federal, State and Local Agencies."
- S. GUARDIAN OF INFORMATION SYSTEMS: Individual ultimately responsible for protecting the security of a particular system and is responsible for ensuring that responsibilities are documented for each site, system and service.
- T. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY (HIPAA): a federal law passed in 1996 that limits restrictions that a group health plan can place on benefits for preexisting conditions, while establishing national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions of the act also added new standards for the security and privacy of health related personal data.

- U. HIPAA UNIT: Agency Unit responsible for managing account management and access control in accordance with relevant Federal, State, and Agency policy.
- V. INCIDENTAL CONTACT: contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.
- W. INDIVIDUAL: the subject of the CPI or the subject of the CPI's authorized representative, legal counsel, legal custodian or legal guardian, and anyone as otherwise permitted under state or federal law acting on behalf of, or in furtherance of, the interests of the subject of the CPI. Individual does NOT include an opposing party in litigation, or the opposing party's legal counsel, or an investigator, auditor or any other party who is not acting on behalf of, or in furtherance of the interests of, the subject of the CPI, even if such individual has obtained a signed release from the subject of the CPI.
- X. INFORMATION OWNER: the one individual appointed in accordance with section 1347.05(A) of the Revised Code to be directly responsible for a system.
- Y. INFORMATION SECURITY: Information is a key organizational asset, Information Security is ensuring the availability, integrity and confidentiality of products and services, while preventing and minimizing security incidents.
- Z. INFORMATION AND TECHNOLOGY SERVICES (ITS): The Unit in ODM responsible for Information Technology (IT) operations.
- AA. INTEGRITY: Safeguarding the accuracy and completeness of information and computer software.
- BB. ITS SERVICE DESK: Unit in ITS responsible for receiving, directing and in some cases resolving end user complaints, problems, and requests.
- CC. ITS INFORMATION SECURITY TEAM: Agency Unit person responsible for ensuring that appropriate organizational security standards, policies, and procedures are developed to support the IPP 3001 Information Security Policy.
- DD. INFORMATION SECURITY LIASON (ISL): Individual designated in the ODM Business unit to interface with the ITS Information Security Team.
- EE. INFORMATION TECHNOLOGY REQUEST FORM (ITR): detailed software request form for new software including title and justification.
- FF. NON-REPUDIATION: Refers to the state of affairs where the purported maker of a statement, action, or contract will not be able to successfully challenge the validity of the statement, action or contract.
- GG. PERSONAL CALL: Any incoming or outgoing call that is not directly related to the performance of an employee's job duties.

- HH. PERSONAL LONG DISTANCE CALL: Any incoming or outgoing call that results in a long distance charge to the State of Ohio that is not related to the performance of an employee's job duties.
- II. PRIVACY IMPACT ASSESSMENT (PIA): To ensure privacy is considered for all information systems, applications, and processes, state agencies are required to create privacy impact statements in accordance with Section 125.18 of the Ohio Revised Code (ORC). A Privacy Impact Assessment (PIA) is the same as a privacy impact statement. Section 1347.15 of the Ohio Revised Code also requires state agencies to complete privacy impact assessment forms.
- JJ. PROGRAM/DATA OWNER: The area identified as being responsible for authorizing entity(s) and level of access to a specific system and/or data. The Program/Data Owner is accountable for authorizing access to the data under their control.
- KK. PROTECTED MEDICAID INFORMATION: data which is protected under the Federal Code of Regulations specific to the Medicaid Program.
- LL. PUBLIC RECORD: data that is subject to disclosure through Ohio public records law section 149.43 of the Revised Code.
- MM. RESEARCH: explore, analyze, or examine data.
- NN. ROUTINE: common place, regular, habitual, or ordinary.
- OO. SECURITY DESIGNEE: Individual, or group, appointed by a particular Program Area as the guardian(s) of the information system(s).
- PP. SOCIAL SECURITY ADMINISTRATION (SSA) DATA: ODM has an agreement with the SSA as an Electronic Information Exchange Partners to receive SSA data for the administration of Medicaid. Data received from the SSA is subject to the requirements of the SSA 'ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES FOR STATE AND LOCAL AGENCIES EXCHANGING ELECTRONIC INFORMATION WITH THE SOCIAL SECURITY ADMINISTRATION.' Information received from the SSA is considered sensitive.
- QQ. SOFTWARE CENTER CONFIGURATION MANAGER: Handles software packaging and deployment.
- RR. SUPERVISOR: An ODM employee(s) who has the responsibility to identify internal employees with the need to access the system, identify the level of access required, submit a formal request, and provide notice of access termination to ODM System Access Management.

- SS. SYSTEM ACCESS MANAGEMENT: Identifies the section within ODM responsible for granting, requesting, provisioning, de-provisioning and/or revoking access to systems under the control of ODM.
- TT. SYSTEM DEVELOPERS: ITS Team(s) or contract resources responsible for the development of each information system or service.
- UU. SYSTEM OR INFORMATION SYSTEMS: As defined in ORC 1347.01, "system" means any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved using the person's name or by an identifying number, symbol, or other identifier assigned to the person. "System" includes both records that are manually stored and records that are stored using electronic data processing equipment. "System" does not include collected archival records in the custody of or administered under the authority of the Ohio Historical Society, published directories, reference materials or newsletters, or routine information that is maintained for the purpose of internal office administration, the use of which would not adversely affect a person.
- VV. SYSTEM OWNER: The designated ODM entity that is the owner of an information system, information system component, or application. Typically this is the development unit supervisor for the specific information system.
- WW. TELEPHONE: Unless otherwise stated, telephone includes both wired telephones and/or Voice over IP telephones (Phones that use the same network and connections as PCs).
- XX. THIRD PARTY: An entity, organization or individual external to ODM.
- YY. UPGRADE: a substantial redesign of an existing system for the purpose of providing a substantial amount of new application functionality, or application modifications which would involve substantial administrative or fiscal resources to implement. "Upgrade" does not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or legal requirements. For the purposes of this policy ODM defines "substantial redesign" to mean any change that modifies greater than 50% of the code in an existing application.
- ZZ. VOIP TELEPHONE SERVICES: Voice over IP telephones with local and long distance telephone service.
- AAA. WIRED TELEPHONE: Traditional hard-wired telephone with local and long distance telephone service.

BBB. WIRELESS TELEPHONE SERVICES: Cellular Telephone: Cellular/wireless telephone and or cellular/wireless device (iPhones, Android phones, Wireless Tablets or WLAN cards) capable of data interface (i.e., email, contacts, and applications).

APPOINTING AUTHORITY APPROVAL <i>John B. Maroney/jbd</i>	POLICY NUMBER ODM/IPP-3925 VERSION 1
	EFFECTIVE DATE July 1, 2015

I. PURPOSE:

To establish departmental requirements for business appropriate uses of ODM Confidential Personal Information (CPI) stored in ODM maintained computer systems. These expectations are based on federal and state statutory requirements.

II. REFERENCE/AUTHORITY:

A. REFERENCES

1. [Ohio Revised Code \(ORC\) 5160.03](#)
2. [Ohio Revised Code \(ORC\) 1347.15](#)
3. [Ohio Revised Code \(ORC\) 1347.12](#)
4. ODM IPP 3001 Information Security Policy
5. ODM IPP 3922 Code of Responsibility

B. AUTHORITY

1. This policy is established by order of the director, ODM, hereinafter referred to as director.
2. Per ORC [5160.03](#), all duties conferred on the various work units of the department by law or by order of the director shall be performed under such rules as the director prescribes and shall be under the director's control.

III. SCOPE:

This policy applies to all state employees in the employment of ODM.

IV. DEFINITIONS:

See Appendix A: IT Glossary

V. POLICY:

The ODM mission is to provide accessible and cost effective health care coverage for Ohioans by promoting personal responsibility and choice through transformative and coordinated quality care.

The ODM mission cannot be achieved without access to the Confidential Personal Information with which our clients and business partners have entrusted us. It is in the interest of maintaining and ensuring this trust that this policy seeks to establish the valid reasons for accessing these key information assets. The computer systems used in the delivery of services are large and complex in nature, as are the back-end data repositories that drive these systems. This makes for an extremely large array of confidential information that we are responsible for maintaining and protecting within these systems. Without this data, we could not function as an organization. Thus, anything that represents a threat to the security of this data, represents a threat to ODM ability to provide services. For this reason each employee must understand their vested interest in maintaining the security and privacy of the confidential information with which we have been entrusted. The purpose of the following is to provide clear guidance as to what is deemed valid access to ODM CPI and the legal basis for this guidance.

A. Criteria for accessing confidential personal information

1. The statutory definition of "CPI" is any personal information that is not considered public record under ORC 149.43. For ODM, CPI includes any non-public information about ODM employees, contractors and service providers (such as social security numbers and non-work-related addresses), as well as any information identifying applicants for, recipients of, and participants in Medicaid and other types of medical assistance.
2. ODM personal information systems are managed on a need to know basis, whereby each information owner determines the level of access required for an employee of the agency to fulfill his or her job duties. The determination of access to CPI must be approved by the employee's supervisor and the information owner prior to providing the employee with access to CPI within a personal information system. ODM has procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties, including but not limited to a transfer or termination. Whenever an employee's job duties no longer requires access to confidential personal information in a personal information system, then that employee's access to CPI shall be removed.

B. VALID REASONS FOR ACCESSING CPI

In general, any access to and use of CPI that is collected and maintained by ODM is strictly limited to those purposes authorized by ODM, and as directly related to the system user's official job duties and work assignments for, and on behalf of, ODM and/or a federal oversight agency. Some examples of when accessing CPI is prohibited include, but are not limited to, access that results in personal or political gain, and commercial use unrelated to official departmental business. Below is a list of valid reasons for accessing CPI (regardless of whether the CPI is maintained electronically or on paper).

1. In the course of administering or performing job duties related to the following processes, authorized employees of the agency would have valid reasons for accessing CPI:
 - a. Responding to (a) public records requests, when public records are comingled with CPI, or (b) records requests made by the individual for his/her own CPI;
 - b. Program administration, including (a) compliance with federal/state laws and regulations, (b) processing or payment of claims, (c) eligibility determinations (d) audits, investigations and oversight, (e) licensing and certification, and (f) administrative hearings;
 - c. Litigation (including discovery and responding to court orders and subpoenas);
 - d. Human resource matters (e.g. hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, time card approvals/issues);
 - e. Complying with an Executive Order or policy;
 - f. Complying with an agency policy or a state administrative policy issued by the Department of Administrative Services, the Office of Budget and Management or other similar state agency;
 - g. Research in the furtherance of agency specific programs in so far as allowed by statute; or
 - h. Complying with a collective bargaining agreement provision.
2. In addition to the general processes described in paragraph (A) above, ODM must comply with numerous federal and state laws and regulations that limit its use and disclosure of CPI, including but not limited to:
 - a. 45 CFR Parts 160 and 164 (HIPAA-45 CFR 164.501);
 - b. 42 CFR 431.300 through 431.307 (Medicaid);
 - c. 5 USC 552a (Social Security Data);
 - d. Ohio Revised Code (ORC) sections:
 - (1) 5101.27 through 5101.31],
 - (2) 5101.99 (penalties for disclosure)
3. Intentional violations of this policy shall result in disciplinary action up to and including removal in accordance with current disciplinary guidelines.

VI. PROCEDURES:

- A. Any upgrades to existing ODM computer systems, or the acquisition of any new computer systems, that stores, manages, or contains Confidential Personal Information (CPI), shall include a mechanism for recording specific access by users of the system to CPI contained within that system. A systems upgrade is defined as any update requiring over half of the lines of code to be modified.
- B. Until an upgrade or new acquisition of the type described above occurs, each Office within ODM is responsible for documenting a manual logging procedure

for their staff. This procedure must be documented and forwarded for review to the ODM Chief Privacy Officer. Upon receipt of the documentation, the ODM Chief Privacy Officer will call upon the ODM Chief of Staff and Chief Legal Counsel or designees to perform a joint review of the manual logging process to validate that it will meet the requirements as set forth in the legislation. This document must show that the process captures the following fields:

1. Employee User Name
2. Date of Access
3. Time of Access
4. Name of Individual (First and Last) whose CPI was access
5. Name of computer system used to access CPI.

C. There exist two exceptions for the need to log access to CPI:

1. The access occurs as a result of research performed for official agency purposes, routine office procedures, or incidental contact with the information, unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals. e.g., a helpdesk staff person is requested to assist in the resolution of a program or technical issue, and in the course of resolving the issue, they must access CPI.
2. The access is to confidential personal information about an individual, and the access occurs as a result of a request by that individual or their legal representative for confidential personal information about that same individual

D. Information Requests

Upon the signed written request of any individual whose confidential personal information may be kept by the agency, the agency shall do all of the following:

1. Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with the confidential personal information.
2. Provide to the individual the confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of chapter 1347 of the Revised Code.
3. During the pendency of an ongoing investigation about the individual, determine what, if any, records can be shared with that individual.

E. Notification of Invalid Access

1. Upon discovery or notification that CPI of a person has been accessed by an agency employee for an invalid reason, the agency shall take steps to notify the person whose information was invalidly accessed as soon as practical and to the extent known at the time. The agency shall delay notification for a period of time necessary to ensure that the notification will not delay or impede an

investigation or jeopardize homeland or national security. The agency may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information invalidly was accessed and to restore the reasonable integrity of the system. "Investigation" as used in this paragraph includes the investigation of the circumstances and involvement of employees surrounding the invalid access of the confidential personal information. Once the agency determines that notification will not delay or impede an investigation, the agency must disclose the access to confidential personal information made for an invalid reason to the subject of the CPI.

2. The notification given by the agency shall inform the person of the type of confidential personal information invalidly accessed and the date(s) of the invalid access (or as closely approximated as possible).
 3. Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.
- F. The ODM director shall designate an employee of the agency to serve as the Data Privacy Point of Contact under the working title of ODM Chief Privacy Officer. The Data Privacy Point of Contact shall work closely with the State of Ohio Chief Privacy Officer, the State Chief Information Security Officer, and the ODM Chief Information Security Officer to assist the agency with both the implementation of privacy protections for the Confidential Personal Information that the agency maintains and compliance with Section 1347.15 of the Revised Code and the rules adopted thereunder.
- G. The ODM Chief Privacy Officer will ensure the timely completion of the Privacy Impact Assessment form developed by the Office of Information Technology.
- H. The Privacy Impact Assessment will be used as a factor to define the security categorization of the information system in the System Security Plan.
- I. The guardian of the information system containing CPI will ensure the system uses encryption and authentication methods commensurate with requirements identified in the Privacy Impact Assessment and documented in the System Security Plan so as to ensure access to CPI is kept secured.
- J. All ODM employees must take part in a departmental training program that will at a minimum include awareness of all applicable statutes, rules, and policies governing access to confidential personal information with which they may come into contact as part of their assigned job duties.

- K. ODM will create a poster describing agency policies related to the protection of confidential personal information and post it in a conspicuous place in the main office of the agency and in all locations where the state agency has branch offices.
- L. Receipt of this policy must be acknowledged by all agency employees.

VII. CONTACT:

Please direct all questions or concerns to IPP_ODM_Policy_Admin@medicaid.ohio.gov.

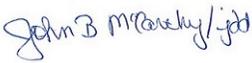
This Policy supersedes any previously issued directive or policy and will remain effective until cancelled or superseded.

VIII. APPENDIX:

A. IT GLOSSARY

IX. REVISION HISTORY:

Date	Description of Change
	Original

APPOINTING AUTHORITY APPROVAL 	POLICY NUMBER: ODM IPP 3927 VERSION 1
	EFFECTIVE DATE: July 29, 2015

I. PURPOSE/REASON:

To define and communicate the procedure for removing access to the Ohio Department of Medicaid (ODM) systems in order that the confidentiality, security and integrity of the personnel that use them and the information they contain may be safeguarded.

II. REFERENCES/AUTHORITY:

A. REFERENCE

1. Ohio Revised Code (ORC) 5160.03.

B. AUTHORITY

1. This policy is established by order of the director, ODM, hereinafter referred to as the director.
2. Per ORC 5160.03, all duties conferred on the various work units of the department by law or by order of the director shall be performed under such rules as the director prescribes and shall be under the director's control.

III. SCOPE:

This procedure applies to all ODM controlled system users including ODM employees, contractors, business associates, external agencies and county employees.

IV. DEFINITIONS:

- A. ACCESS REQUEST – Identifies the section within ODM responsible for the granting or revoking of access to systems under the control of ODM.
- B. AUTHORITATIVE SOURCE – An ODM employee(s) with responsibility to authorize access, identify the level of access, submit a formal request on behalf of the user(s), and provide notice of access termination to ODM Access Request.
- C. PROGRAM/DATA OWNER – The area identified as being responsible for authorizing the level of access to a specific system and/or data. The Program/Data Owner is accountable for authorizing access to the program/data under their control.
- D. EXTERNAL ENTITY - Refers to any non-ODM person or group requesting access to an ODM controlled program/data. External Entities may include business associates, county users, other state and or federal agencies.

V. PROCEDURES:

ODM Managers/Supervisors, ODM Human Resources or other ODM Authoritative Sources are responsible for notifying Access Request of all access terminations.

1. Access Request **must be notified prior to a systems user's last day of employment or as soon as possible for removals from all ODM controlled systems.** This notification may occur in one of the following ways:
 - a. Formal letter
 - b. ODM Exit Information Checklist e-mailed to human resources
 - c. E-mail to accessrequest@medicaid.ohio.gov
The letter/email must include:
 - i. User's first and last name
 - ii. Last day of employment
 - iii. All known User ID's.
 - iv. All known systems to which they have access

2. When account access must be revoked under duress, a person with the authority to request access termination shall notify Human Resources, ITS and system access management control immediately. The notification may be accomplished by:
 - a. In person request
 - b. Telephone
 - c. Red letter email

If request is made in person or by phone, written notification of the request -via email to all parties - must follow.

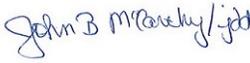
IV. CONTACT:

Please direct all questions or concerns to IPP_ODM_Policy_Admin@medicaid.ohio.gov.

This Policy supersedes any previously issued directive or policy and will remain effective until cancelled or superseded.

V. REVISION HISTORY:

Date	Revision History
	Original

APPOINTING AUTHORITY SIGNATURE 	POLICY NUMBER: ODM IPP 8510 VERSION 1
	EFFECTIVE DATE: July 9, 2015

I. PURPOSE/REASON:

This policy document has been prepared by the Ohio Department of Medicaid (ODM). It is intended to serve as a document of authority relating to the use of Federal Tax Information (FTI) for employees and contractors having ODM system access. It is highly unlikely that employees and contractors will come in direct contact with FTI through the Internal Revenue Service or recognized secondary sources to include the Social Security Administration, Federal Office of Child Support Enforcement or Bureau of Fiscal Services. In the event of unintended access employees and contractors must follow the procedures outlined in this document relating to unauthorized inspection or disclosure under section VI Policy.

II. REFERENCE/AUTHORITY:

A. REFERENCES

1. Ohio Revised Code (ORC) 1347.15
2. Internal Revenue Code §6103, 26 U.S. Code §§ 7213, 7213 A

B. AUTHORITY

1. This policy is established by order of the Director, ODM, hereinafter referred to as Director.
2. Per ORC 5160.02, all duties conferred on the various work units of the department by law or by order of the Director shall be performed under such rules as the Director prescribes and shall be under the Director's control.

III. SCOPE:

This policy applies to all ODM employees or contractors with access to ODM data in any form.

IV. DEFINITIONS:

- A. Federal Tax Information (FTI): FTI is any return or return information received from the Internal Revenue Service or secondary source, such as the Social Security Administration, Federal Office of Child Support Enforcement, or Bureau of Fiscal Services. FTI includes any information created by the recipient that is derived from

- the return or return information. FTI does not include information provided directly by the tax payer or third parties other than those listed above.
- B. Return: The term “return” means any tax or information return, declaration of estimated tax, or, claim for refund required by, or provided for or permitted under this section (26 U.S.C. Section 6103) including supporting schedules, attachments, or lists which are supplemented to, or part of the return.
- C. Return Information: The term “return information” includes a taxpayer’s identity, the nature, source, or amount of income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, or tax payments, whether the tax payer’s return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense. Return information excludes information provided directly by the individual or a third party other than the Internal Revenue Service, Social Security Administration, Federal Office of Child Support, or Bureau of Fiscal Services.

V. POLICY:

- A. In compliance with Internal Revenue Service (IRS) regulations access to FTI is permitted only to individuals who require the FTI to perform their official duties and as authorized under IRS regulations. FTI must never be indiscriminately disseminated internally or externally.
- B. Access to FTI received by ODM for an authorized use may not be used in any manner or for any purpose not consistent with that authorized use.
- C. Unauthorized access or disclosure has been defined as follows:
1. Unauthorized access occurs when an individual receives or has access to FTI without authority. An unauthorized access is willful when it is done voluntarily and intentionally with full knowledge that it is wrong.
 2. Unauthorized disclosure occurs when an individual authorized to receive FTI discloses FTI to another individual or entity who does not have authority and a need to know.
 3. FTI does not include information provided by the taxpayer or third parties, excluding the Social Security Administration, Federal Office of Child Support Enforcement, or Bureau of Fiscal Services.

VI. PROCEDURES:

- A. In the event that an employee or contractor receives access to FTI that has not been specifically assigned to them, or becomes aware of another person inappropriately accessing or disclosing FTI, they must immediately report such access to their supervisor.
- B. The supervisor is responsible for determining whether the source of the FTI is through the IRS or a designated secondary source, such as the Social Security Administration, Federal Office of Child Support Enforcement, or Bureau of Fiscal Services. In the event that the source of the information is unauthorized or undetermined the supervisor must immediately notify the ODM Privacy Official. If the information has been self-disclosed or received from an unrestricted secondary source the supervisor should review the regulations relating to the use and disclosure of CPI with the employee and document their actions.
- C. The Privacy Official will immediately investigate any report received to determine whether improper inspections or disclosures, including breaches and security incidents, have occurred. If it is determined that a breach, security incident, or other inappropriate uses have occurred, the Privacy official will notify the Treasury Inspector General for Tax Administration (TIGTA) and the IRS, Office of Safeguards. The Privacy Official shall notify the TIGTA and IRS immediately, but no later than 24-hours after identification of a possible issue involving FTI. To notify the IRS Office of Safeguards, the Privacy Official should document the specifics of the incident known at that time into a Data Incident Report, including but not limited to:
1. Name of agency and agency point of contact for resolving data incident with their contact information
 2. Date and time of the incident
 3. Date and time the incident was discovered
 4. How the incident was discovered
 5. Description of the incident and the data involved. Include specific data elements if known
 6. Potential number of FTI records involved. If unknown, provide a range if possible.
 7. Address where the incident occurred
 8. Information technology involved (example: laptop, server, mainframe)
 9. Do not include any FTI in the Data Incident report
 10. Email the Data Incident Report to the SafeguardReports@IRS.gov mailbox. Reports should be sent electronically and encrypted via IRS approved encryption techniques. Use the term "Data Incident Report" in the subject line of the email

- D. The ODM Privacy Official will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident. Based upon the analysis of the incident, the agency may be required by the Office of Safeguards to modify security policy, procedure, or controls to more appropriately protect FTI. The Office of Safeguards will coordinate with the agency to ensure appropriate follow-up actions taken by the agency have been completed to ensure continued protection of FTI in the possession of the agency.
- E. Notification to impacted individuals regarding an unauthorized disclosure or data breach incident is based upon the ODM Breach Notification internal policy since the FTI is within the agency's possession or control. However, the agency must inform the IRS Office of Safeguards of notification activities undertaken, preferably before released to the impacted individuals. In addition, the agency must inform the Office of Safeguards of any pending media releases, including sharing the text, prior to distribution.
- F. All employees are required to review this policy on an annual basis.

VII. PENALTIES

- A. ODM employees and contractors found in violation of this policy may be subject to discipline up to and including removal in addition to penalties established under ORC 1347.15(H)(3), which prohibits any state agency from employing any person who has been convicted of or pleaded guilty to a violation of this section. Federal sanctions for unauthorized disclosure or access to FTI are as follows:
 - 1. Willful unauthorized disclosure of FTI by a current or former employee or contractor is a felony subject to a fine of up to \$5,000 or up to five (5) years imprisonment or both.
 - 2. Willful unauthorized access to FTI by a current or former employee or contractor is a misdemeanor subject to a fine up to \$1,000 or up to one (1) year in prison.

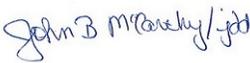
VIII. CONTACT:

Please direct all questions or concerns to IPP_ODM_Policy_Admin@medicaid.ohio.gov.

This Policy supersedes any previously issued directive or policy and will remain effective until cancelled or superseded.

IX. REVISION HISTORY:

Date	Description of Change
	Original

APPOINTING AUTHORITY SIGNATURE 	POLICY NUMBER: ODM IPP 8511 VERSION 1
	EFFECTIVE DATE: August 3, 2015

I. PURPOSE/REASON:

For purposes of documenting employee access to Confidential Personal Information (CPI) accessed through any Ohio Department of Medicaid (ODM) or other state agency interconnected computer system. This IPP is being issued to comply with the Ohio Revised Code section 1347.15.

II. REFERENCE/AUTHORITY:

A. REFERENCES

1. Ohio Revised Code (ORC) 1347.15
2. ORC 1347.01
3. ORC 5160.02
4. Ohio Administrative Code (OAC) 5101:9-22-16

B. AUTHORITY

1. This policy is established by order of the Director, ODM, hereinafter referred to as Director.
2. Per ORC 5160.02, all duties conferred on the various work units of the department by law or by order of the Director shall be performed under such rules as the Director prescribes and shall be under the Director's control.

III. DEFINITIONS:

- A. Confidential Personal Information (CPI): CPI includes all information about an individual kept by any public office, including but not limited to, state, county, village or school district that is not a public record.
- B. System or Information System: As defined in ORC 1347.01, "system" means any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved using the person's name or by an identifying number, symbol, or other identifier assigned to the person. "System" includes both records that are manually stored and records that are stored using electronic data processing equipment.
- C. Interconnection of Systems: Refers to a linking of systems that belong to more than one agency, or to an agency and other organizations, which linking of systems results

in a system that permits each agency or organization involved in the linking to have unrestricted access to the systems of the other agencies and organizations.

IV. SCOPE:

This policy applies to all ODM employees accessing CPI through the use of an ODM or other state agency interconnected computer system if the system does not contain a mechanism to track access to CPI by specific ODM employee and report the access upon request.

This policy does not apply to CPI access when (1) access to CPI is requested by the subject of the CPI, the subject's guardian or the subject's authorized representative or anyone as otherwise permitted under state or federal law acting on behalf of, or in furtherance of the interests of the subject of the CPI; or (2) the access to CPI occurs as a result of research performed for official ODM purposes, including the performance of activities related to the administration of the state plan or routine office procedures, or research that results in incidental contact with CPI.

V. REQUIREMENTS:

A. Prerequisites

1. ODM has adopted rules under Chapter 119 of the Revised Code including OAC 5101:9-22-16, regulating employee access to CPI pursuant to section 1347.15 of the Revised Code.
2. It has been determined by the ODM Office of Information and Technology Services that the computer system(s) being used by ODM employees to access CPI does not contain a mechanism to track access to CPI nor can it electronically issue a report showing: the date of access, identity of the person(s) whose CPI was accessed and the ODM employee who accessed the CPI.

B. Expected Performance

1. An ODM employee accesses CPI through an ODM or other state agency interconnected computer system that does contain a mechanism to track access.
 - a. The ODM employee must determine who requested the CPI be accessed and why. If access to the CPI is due to the following; the ODM employee does not have to proceed any further or take any further action pursuant to this procedure:
 - i. Access is as a result of a request from the subject of the CPI, the subject's guardian or the subject's authorized representative or anyone as otherwise permitted under state or federal law acting on behalf of or in furtherance of the interests of the subject of CPI. Acting on behalf of or in furtherance of the interests of, the subject of the CPI does NOT include an opposing party in litigation, or the opposing parties'

legal counsel, or an investigator, auditor or other third party, even if the individual has obtained a signed release from the subject of the CPI.

- ii. Access to the CPI is a result of research performed for official ODM purposes or routine office procedures, or that results in incidental contact with the CPI; unless the conduct resulting in the access is specifically directed toward a specifically named individual or a group of specifically named individuals.
2. If access to the CPI does not fall within the above exceptions then the ODM employee must complete the following process for each separate CPI access (VII)

VI. PROCEDURES:

- A. Create a log entry utilizing the Confidential Personal Information Log (CPILOG) desktop icon and application that contains the ODM employee’s name, identifying information for the subject of the CPI accessed, and the date the CPI was accessed. Logging must occur at the time of access or as soon as reasonably practical.
- B. Employees are directed to consult their supervisor if questions arise regarding the need to log inquiries.
- C. Employee CPILOG entries are subject to supervisor review to assure compliance.

VII. PENALTIES

ODM employees found in violation of this policy may be subject to ODM disciplinary procedures under ORC 1347.15(H)(3), which prohibits any state agency from employing any person who has been convicted of or pleaded guilty to a violation of this section.

VIII. CONTACT:

Please direct all questions or concerns to IPP_ODM_Policy_Admin@medicaid.ohio.gov.

This Policy supersedes any previously issued directive or policy and will remain effective until cancelled or superseded.

IX. REVISION HISTORY:

Date	Revision History
	Original

(Current as of August 6, 2015)

- A. **AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI):** A private, non-profit organization that administers, coordinates, and accredits the U.S. voluntary standardization and conformity assessment system. HIPAA prescribes that the standards mandated under it be developed by ANSI accredited bodies whenever practical.
- B. **BREACH:** The acquisition, access, use or disclosure of Protected Health Information (PHI) in a manner which compromises the security or privacy of the PHI. For purposes of this definition, “compromises the security or privacy of PHI” means that the acquisition, access, use or disclosure poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include names; date of birth, zip code; postal address information, other than town or city, State, and zip code; telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images; is not considered to compromise the security or privacy of the subject of the PHI.
1. Breach excludes: (1) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or a Business Associate (BA), if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA: (2) Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA: or (3) A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- C. **BUSINESS ASSOCIATE (BA):** (1) Except as provided in paragraph (2) of this definition, BA means, with respect to a CE, a person who:(i) On behalf of such CE or of an organized health care arrangement in which the CE participates, but other than in the capacity of a member of the workforce of such CE or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or

administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or (B) Any other function or activity regulated by HIPAA privacy regulations; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in Sec. 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement. (3) A covered entity may be a business associate of another covered entity.

- D. **CLAIM ADJUSTMENT REASON CODES:** A national administrative code set that identifies the reasons for any differences, or adjustments, between the original provider charge for a claim or service and the payer's payment for it.
- E. **CLAIM ATTACHMENT:** Any of a variety of hard-copy forms or electronic records needed to process a claim in addition to the claim itself.
- F. **CODE SET:** Under HIPAA, this is any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. This includes both the codes and their descriptions.
- G. **CODE SET MAINTAINING ORGANIZATION:** Under HIPAA, this is an organization that creates and maintains the code sets adopted by the U.S. Department of Health and Human Services (HHS) for use in the transactions for which standards are adopted.
- H. **COORDINATION OF BENEFITS (COB):** A process for determining the respective responsibilities of two or more health plans that have some financial responsibility for a medical claim. Also called “cross over”.
- I. **COVERED ENTITY (CE):** A health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.

-
1. HEALTH PLAN: An individual plan or group plan that provides, or pays the cost of, medical care.
 - a. Health plan includes: The following, singly or in combination:
 - 1) A group health plan.
 - 2) A health insurance issuer.
 - 3) An HMO.
 - 4) Part A or Part B of the Medicare program under title XVIII of the Act.
 - 5) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
 - 6) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).
 - 7) An issuer of a long term care policy, excluding a nursing home fixed indemnity policy.
 - 8) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
 - 9) The health care program for active military personnel under title 10 of the United States Code.
 - 10) The veteran's health care program under 38 U.S.C. chapter 17.
 - 11) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).
 - 12) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.
 - 13) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
 - 14) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
 - 15) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w 21 through 1395w 28.
 - 16) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
 - 17) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the Public Health Service (PHS) Act, 42 U.S.C. 300gg 91(a)(2)).
 - b. Health plan excludes: (i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg 91(c)(1); and (ii) A government funded program (other than one listed in paragraph (1)(i) (xvi) of this definition): (A) Whose principal purpose is other than providing, or paying the

-
- cost of, health care; or (B) Whose principal activity is:(1) The direct provision of health care to persons; or (2) The making of grants to fund the direct provision of health care to persons.
2. HEALTH CARE CLEARINGHOUSE: A public or private entity, including a billing service, re-pricing company, community health management information system or community health information system, and "value added" networks and switches, that does either of the following functions:
- a) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
 - b) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
3. Health care provider: A provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
- J. Covered Functions: Those functions of a CE, the performance of which make the entity a health plan, a health care clearinghouse or a health care provider.
- K. CURRENT PROCEDURAL TERMINOLOGY (CPT): It refers to a regularly updated "book" of procedure codes which all medical providers, private and public, use.
- L. DESIGNATED CODE SET: A medical code set or an administrative code set that HHS has designated for use in one or more of the HIPAA standards.
- M. DESIGNATED RECORD SET: A group of records maintained by or for a CE that is: the medical and billing records relating to an individual maintained by or for a health care provider; the enrollment, payment, claims adjudication and case or medical management systems maintained by or for a health plan; or used, in whole or part, by or for a CE to make decisions about individuals.
- N. DESIGNATED STANDARD MAINTENANCE ORGANIZATION (DSMO): An organization that the Secretary, HHS, has designated to maintain the standards; receive and process requests for adopting a new standard or modifying an adopted standard.
- O. ELECTRONIC DATA INTERCHANGE (EDI): This usually means certain variable length formats for the electronic exchange of structured data. It is sometimes used more broadly to mean any electronic exchange of formatted data.

-
- P. CENTERS FOR MEDICARE AND MEDICAID SERVICES (CMS): Formerly known as the Healthcare Financing Administration (HCFA), CMS is the primary federal agency overseeing the funding, regulation and administration of the Medicaid program by the states. NOTE: some of the acronyms associated with CMS continue to contain HCFA.
- Q. HCFA COMMON PROCEDURAL CODING SYSTEM (HCPCS): A medical code set that identifies health care procedures equipment, and supplies for claim submission purposes. It has been selected for use in the HIPAA transactions. HCPCS Level I contains numeric CPT codes which are maintained by the American Medical Association (AMA). HCPCS Level II contains alphanumeric codes used to identify various items and services that are not included in the CPT medical code set.
- R. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA): A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives the U.S. Department of Health and Human Services (HHS) the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of PHI as defined under the Act. Also, known as the Kennedy Kassebaum Bill, K2, or Public Law 104-191.
- S. HEALTH LEVEL SEVEN (HL7): An ANSI accredited group that defines standards for the cross platform exchange of information within a health care organization. HL7 is responsible for specifying the Level Seven OSI standards for the health industry.
- T. HEALTH OVERSIGHT AGENCY: A governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is authorized by law to oversee the public or private health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights for which health information is relevant.
- U. HYBRID ENTITY: A single legal entity that is a CE whose covered functions are not its primary functions. This single entity must designate its health care component(s) that would have met the definition of CE under HIPAA had the component(s) been

- separate from the entity. Health care components of the entity also may include any component only to the extent it performs covered functions or activities that would make such component a BA of another entity component that performs covered function(s) if the two components of the entity were separate legal entities.
- V. **INDIRECT TREATMENT RELATIONSHIP:** A relationship between an individual and a health care provider in which the health care provider delivers health care to the individual based on the orders of another health care provider and the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.
- W. **J CODES:** A subset of the HCPCS Level II code set with a high order value of "J" that has been used to identify certain drugs and other items.
- X. **LAW ENFORCEMENT OFFICIAL:** A public employee from any branch of government who is empowered by law to investigate a potential violation of the law or to prosecute, or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- Y. **LOCAL CODE(S):** A generic term for code values that are defined for a state or other political subdivision, or for a specific payer. This term is most commonly used to describe HCPCS Level III Codes, but also applies to state assigned Institutional Revenue Codes, Condition Codes, Occurrence Codes, Value Codes, etc.
- Z. **NATIONAL ASSOCIATION OF STATE MEDICAID DIRECTORS (NASMD):** An association of state Medicaid directors. NASMD is affiliated with the American Public Health Human Services Association (APHSA). The Nation Medicaid EDI HIPAA (NMEH) has been implemented under this organization to work on the EDI related HIPAA provisions.
- AA. **NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS (NCVHS):** A Federal advisory body within HHS that advises the Secretary regarding potential changes to the HIPAA standards.
- BB. **NATIONAL EMPLOYER ID:** A system for uniquely identifying all sponsors of health care benefits.
- CC. **NATIONAL UNIFORM BILLING COMMITTEE (NUBC):** An organization, chaired

and hosted by the American Hospital Association, that maintains the UB 92 institutional billing paper form or its electronic equivalent. The NUBC has a formal consultative role under HIPAA for all transactions affecting institutional health care services.

- DD. NATIONAL UNIFORM CLAIM COMMITTEE (NUCC): An organization, chaired and hosted by the American Medical Association, that maintains the HCFA 1500 claim paper form or its electronic equivalent, the Professional EMC NSF, and the X12 837. The NUCC also maintains the Provider Taxonomy Codes and has a formal consultative role under HIPAA for all transactions affecting non dental non institutional professional health care services.
- EE. OFFICE FOR CIVIL RIGHTS: The HHS entity responsible for enforcing HIPAA including but not limited to investigations of HIPAA violations, imposition of corrective action plans in response to HIPAA violations and ability to utilize collected HIPAA related civil money penalties to further its responsibilities involving HIPAA enforcement.
- FF. PERSONAL REPRESENTATIVE: A person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting in loco parentis who is authorized under law to make health care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or other person acting in loco parentis has assented to an agreement of confidentiality between the provider and the minor.
- GG. PRIMARY INFORMATION PERSON (PIP): The head of household or assistance group.
- HH. PROTECTED HEALTH INFORMATION (PHI): Individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual. PHI does not include certain education records specified in Title 20 of the United States Code at section 1232g; and employment records held by a CE in its role as an employer.
- II. PROVIDER TAXONOMY CODES: An administrative code set for identifying the provider type and area of specialization for all health care providers. A given provider can have several Provider Taxonomy Codes. This code set is used in the Referral Certification and Authorization and Claim transactions, and is maintained by the NUCC.

- JJ. PUBLIC HEALTH AUTHORITY: A governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is responsible for public health matters as part of its official mandate.
- KK. RESEARCH: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
- LL. RECIPIENT: Includes any individual receiving benefits under a program administered by the Ohio Department of Medicaid (ODM). To the extent appropriate in the context, "recipient" includes an individual applying for an ODM-administered program, a former recipient, or both.
- MM. STANDARD TRANSACTION: Under HIPAA, this is a transaction that complies with the applicable HIPAA standard.
- NN. STANDARD SETTING ORGANIZATION (SSO): This is an organization accredited by ANSI that develops and maintains standards for information transaction or data elements, or any other standard necessary to implement the Electronic Transaction rule.
- OO. TRADING PARTNER AGREEMENT (TPA): Under HIPAA, this is an agreement related to the exchange of information in electronic transaction, whether the agreement is distinct or part of a larger agreement, between each party to the agreement.
- PP. TRANSACTION: Under HIPAA, this is the exchange of information between two parties to carry out financial or administrative activities related to health care.
- QQ. TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS (TPO): Includes all of the following:
1. TREATMENT: The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
 2. PAYMENT:
 - a. The activities undertaken by:
 - 1) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan;

-
- 2) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
 - b. The activities in paragraph 1 of this definition relate to the individual to whom health care is provided and include, but are not limited to:
 - 1) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
 - 2) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
 - 3) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop loss insurance and excess of loss insurance), and related health care data processing;
 - 4) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
 - 5) Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services;
 - 6) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement.
 3. **HEALTH CARE OPERATIONS:** Means any of the following activities of the covered entity to the extent that the activities are related to a covered function:
 - a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
 - b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non health care professionals, accreditation, certification, licensing, or credentialing activities;
 - c. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop loss insurance and excess of loss insurance), provided that the requirements of Sec.164.514(g) are met, if applicable;

- d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- e. Business planning and development, such as conducting cost management and planning related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
- f. Business management and general administrative activities of the entity, including, but not limited to:
 - 1) Management activities relating to implementation of and compliance with the requirements of this subchapter;
 - 2) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
 - 3) Resolution of internal grievances;
 - 4) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
 - 5) Consistent with the applicable requirements of Sec. 164.514, creating de identified health information or a limited data set, and fundraising for the benefit of the covered entity.

RR. VALUE ADDED NETWORK (VAN): A vendor of EDI data communications and translation services.

SS. WORKFORCE: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a CE, is under the direct control of such entity, whether or not they are paid by the entity