MICHIGAN DEPARTMENT OF HEALTH AND HUMAN SERVICES • STATE UNIT ON AGING
Bureau of Aging, Community Living, and Supports

AGING INFORMATION SYSTEM (AIS) INFORMATION TECHNOLOGY (IT) SECURITY GUIDE

Policies, Procedures, and Best Practices

CONFIDENTIAL • *For AIS Users Only*

Version 1.0 • 2025

CONTENTS

1.0 Introduction 1
2.0 Compliance Requirement 1
3.0 The Aging Information System (AIS) 2
4.0 AIS Data Protection and Security 3
5.0 Acceptable Use of AIS Data and Systems 4
6.0 AIS Security Incident Reporting 5
6.1 Reportable AIS Security Incidents 5
6.2 Incident Response Procedure 6
7.0 Password Account Management 7
8.0 Storage of AIS Data on Personal Mobile Devices 8
9.0 Use of Privately Owned Portable Devices 8
10.0 Record Management: Disposal and Retention 9
11.0 Vendor User Administration 10
12.0 User Verification Audit 10
13.0 Electronic Signature 11
14.0 AIS User Roles and Training 12
14.1 AIS User Roles 12
14.2 AIS Training 12
15.0 Agency IT Security Officer 13
16.0 Emergency Prepardness And Disaster Recovery 14
17.0 Acknowledgment of Receipt 16
18.0 Best Practices 17
Documents 18
Acronyms 19
Terms and Definitions 20
Revision History 23

1.0 INTRODUCTION

As Michigan's State Unit on Aging (SUA), the Bureau of Aging, Community Living, and Supports (ACLS Bureau), is responsible for maintaining Information Technology (IT) security for the Aging Information System (AIS). In compliance with the Older Americans Act, Federal and state laws, the ACLS Bureau has established policies and procedures to safeguard AIS information and information systems.

This Guide outlines the security policies and procedures for the internet-based AIS Partner Channel and Business Site networks and applications. Its goal is to provide authorized AIS Users with guidance on the proper use of the State of Michigan (SOM) AIS technology resources. AIS Users are obligated to review the policies and guidelines contained in this guide on a regular basis. These policies remain in effect until superseded or rescinded by the ACLS Bureau. *This Guide replaces Transmittal Letter 436 dated 12/06/2004.*

AIS information is not limited to data in computer systems and should be protected wherever it is kept in an agency, no matter what form it takes, (electronic, printed, etc.), whatever technology is used to handle it, or whatever purpose it serves. The SOM has established Information Technology security policies, standards, and procedures in accordance with the National Institute of Standards and Technology (NIST). Any AIS data that originated, entered, processed, transmitted, stored or disposed of for the AIS is considered SOM information.

- **DTMB - Information Technology Policies, Standards & Procedures**
  (https://www.michigan.gov/dtmb/policies/it-policies)

2.0 COMPLIANCE REQUIREMENT

To ensure adherence to the AIS IT security policies, procedures and practices all AIS Users having access to AIS Partner Channel and Business Site applications must comply with all policies and procedures contained in this Guide and with applicable SOM Technical Standards or Procedures. In addition, all AIS Users must comply with Federal and State cyber security laws and regulations. Any misuse or violation of these policies or technical standards must be promptly reported.

When logging into the AIS Partner Channel, AIS Users are required to accept the Terms and Conditions, acknowledging receipt of the AIS IT Security Guide, before gaining access to the system. Acceptance confirms that the AIS User has received a copy of the Guide.

Non-compliance or violation of the policies or procedures described in this Guide could result in civil or criminal penalties. Exceptions to these policies or procedures must be approved, as required, by the ACLS Bureau.

3.0 THE AGING INFORMATION SYSTEM (AIS)

AIS is a modest technology platform developed to collect programmatic data and information on Michigan's older adult population. Protecting AIS applications and data from cyber-attacks is challenging in today's globalized threat environment.

The Aging Information System, AIS, consists of two Internet-based networks: (i) Partner Channel and (ii) Business Site, that function independently to collect, report, and analyze statewide aging services data. These two sites are considered State of Michigan (SOM) Information Technology (IT) systems.

The **Partner Channel** houses 30 software modules designed to collect Older Americans Act data and program information and trends of the older adult population in Michigan. Partner Channel access is limited to individuals with a legitimate need to access AIS applications.

The **Business Site** supports business operations for service providers and network users. In addition, the Site maintains program materials and resources for Partner Channel users and Aging Network partners. This is a private non-searchable Internet site which is accessible to Area Agencies on Aging, Volunteer Program and Aging Network partners that possess the URL https://www.osapartner.net.

AIS Network	Internet URL	Supported Browsers
AIS Partner Channel ***Houses 30 Internet-based applications that support data collection and reporting for Michigan's Aging Network***	**ais.osapartner.net**	• *Microsoft Edge* • *Mozilla Firefox* • *Google Chrome*
AIS Business Site ***Houses Partner Channel companion applications and information and resources for aging programs and network providers***	**www.osapartner.net**	

4.0 AIS DATA PROTECTION AND SECURITY

The purpose of this policy is to maintain safeguards and procedures to protect and secure AIS data and applications from unauthorized, disclosure, modification, access, use, destruction, and the loss or delay in service. AIS operations depend on a secure network to ensure the AIS infrastructure remains intact and protected from cyber threats.

This policy is established in accordance with the SOM Policy 1304.00 Information Technology Information Security. *This policy statement replaces Transmittal Letters 195 and 436.*

POLICY STATEMENT ..... Data Protection and Security

4.1 AIS Users will not attempt to disrupt the information security of the AIS network.

4.2 AIS Users must ensure AIS data is accessed in a secure environment.

4.3. AIS Users must comply with applicable Federal and State cyber security laws and regulations.

4.4 Only employees designated by the provider agency may make entries in the service recipient's record.

4.5 Systems and devices storing AIS information, even for a limited duration, must be encrypted in compliance with the applicable standards in the SOM Technical Standard 1340.00.170.03 Electronic Data Encryption.

4.6 Must not disclose sensitive data to any unauthorized person without the documented permission unless part of legitimate job duties.

4.7 Agencies must maintain the accuracy and completeness of data for which they are responsible whether that data is contained in a centrally managed system or in a locally managed system.

4.8 AIS data and information shall not be downloaded and stored on personal devices.

4.9 AIS data must never be put into artificial intelligence (AI) systems.

4.10 Providing unauthorized persons with any information that is sensitive or protected by law; unauthorized posting of AIS information and data to external newsgroups, bulletin boards, or other public forums; and storing AIS information in public storage services without approval from the ACLS Bureau is prohibited.

4.11 All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less.

4.12 When AIS sessions are active, AIS Users must lock down their PCs, laptops, and workstations by locking (control-alt-delete) when devices will be unattended for any amount of time.

4.13 AIS Users must never access another AIS User's account and/or misrepresent one's identity.

4.14 AIS Users must never allow another person to access their account or share their password.

4.15 The use of AIS data and sensitive information outside of normal program management activities shall require the implementation and documentation of a ***Data Sharing Agreement*** between the agency and the recipient. Below are examples of AIS data requiring implementation of a Data Sharing Agreement include, but are not limited to:

(i) AIS data populated on non-AIS information systems (e.g., local service provider National Aging Program Information System (NAPIS) data collection systems).

(ii) Analysis/use of AIS data where data will be extracted and stored on non-AIS systems.

(iii) Access and use of AIS data by non-authorized users acting on behalf of an authorized AIS agency (e.g., statistical analysis conducted on behalf of an AIS agency under a contract with a researcher, etc.).

(iv) If the data being shared is used in future publications the SOM should be acknowledged.

(v) Data Sharing Agreements shall be retained at the Agency level according to SOM document retention and storage guidelines.

5.0 ACCEPTABLE USE OF AIS DATA AND SYSTEMS

The purpose of this policy is to provide AIS Users with guidance on the acceptable use of AIS data and information systems. This policy protects both authorized AIS Users and AIS by ensuring that services are used appropriately. Moreover, these policies provide a framework for monitoring and enforcing compliance.

In addition to this policy, AIS Users must comply with the applicable SOM Technical Standard 1340.00.130.02 Acceptable Use of Information Technology.

POLICY STATEMENT ..... Acceptable Use of AIS Data

5.1 It is prohibited to use AIS data, information technology and resources for personal gain.

5.2 The AIS applications, reports, electronic files, and data may only be used for lawful purposes.

5.3 AIS Users must not attempt to disrupt the information security of the AIS network.

5.4 Dissemination of AIS data to unauthorized external parties is prohibited.

5.5 AIS data and information must be stored securely, and data is accessed in a secure environment.

5.6 Intentionally introducing computer viruses, worms, Trojan Horses, or other rogue programs into AIS information technology resources is in violation of this policy and is punishable by law.

5.7 Using or encouraging others to use AIS information technology resources in a manner that violates this policy, or any applicable state or federal law is prohibited.

5.8 Electronic files containing AIS client data and information, whether created, sent, received, or stored are SOM property and may be accessed by appropriate ACLS Bureau personnel.

5.9 When applicable, a Data Sharing Agreement must be established when sharing AIS data. See section 4.0.

5.10 AIS Users acknowledge that disciplinary action may be imposed if this policy is violated.

6.0 AIS SECURITY INCIDENT REPORTING

The purpose of this policy is to define the Incident Response Reporting procedures in the event of an actual or suspected AIS information security incident. This policy aims to outline the process of reporting information technology security threats to the ACLS Bureau and AIS IT vendor. Further, its goal is to ensure that all parties are aware of their responsibilities regarding IT system security incident reporting.

6.1 Reportable AIS Security Incidents

An AIS security incident is defined as any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, interference with information technology operation of the AIS Partner Channel or Business Site applications and data. Any real or perceived activity that could result in a breach of confidentiality, security, and/or disrupt/corrupt AIS data, databases, operations, and hardware and software applications, is a reportable security incident.

AIS Users are required to report any activities that meet the criteria for security incidents to the ACLS Bureau and ACRO Service Corporation. Attachment C identifies programs, agencies, and organizations in the Aging Network affected by this policy.

The following types of activities are examples of AIS security incidents that must be reported:

- *Attempts (either failed or successful) to gain unauthorized access to AIS applications, data, and databases.*
- *Any suspected access to AIS applications by unauthorized persons.*

- *Unauthorized use of AIS information that is required to be kept confidential.*
- *Attempts to introduce a computer-related contaminant (e.g., malicious code, virus, worm, etc.) in the AIS.*
- *Receipt of an extortion message threatening to perpetrate a cyber-attack.*
- *The loss or theft of a computing device that stores AIS.*
- *Unwanted disruption or denial of AIS service.*
- *Unauthorized use of the AIS for transmission, processing, or storage of data.*
- *Changes to AIS hardware, software, data, or database applications.*
- *Attempts to alter, damage, or destroy any AIS applications, databases, or data.*
- *Reckless or intentional attempts to disrupt any AIS operations or denial of service attacks.*

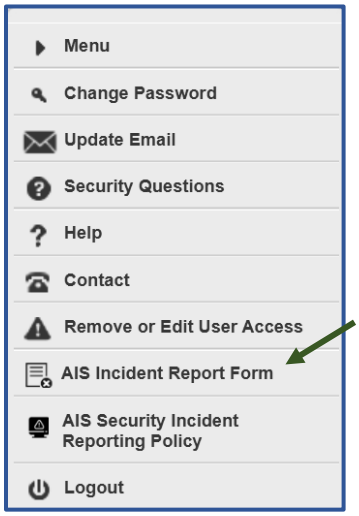
6.2 Incident Response Procedure

AIS security incidents, whether suspected or real, must be reported immediately to the ACLS Bureau and ACRO Service Corporation. The following methods are available to report security incidents:

(i) An Online Incident Report can be submitted via the Partner Channel Home Page. This form can be completed online and electronically submitted to the AIS IT Security Team.

(ii) The AIS Incident Report Form can be downloaded from the AIS Business Site at www.osapartner.net. See section AIS Forms. Also, a fillable form is included in the Documents section of this guide.

(iii) Forward the completed Incident Report via email to: **MDHHS-AIS-SECURITY@michigan.gov**.



AIS security notification and concerns can be made via telephone or e-mail during and after normal business hours. Leave a detailed message if there is no initial response.

Phone and e-mail contact numbers:

517-241-4100 SOM ACLS Bureau
248-755-0485 ACRO Services Corporation

AIS IT Security E-mail Address
MDHHS-AIS-SECURITY@michigan.gov

In addition to this policy, AIS Users must comply with the applicable SOM Technical Standard 1340.00.090.01 Incident Response**.** *This policy replaces Transmittal Letter 2007-151.*

POLICY STATEMENT ..... Security Incident Reporting

6.1 All Users of AIS IT resources must report security incidents immediately or within 24 hours to the ACLS Bureau and ACRO Service Corporation. Additionally, users should contact their organization's Information Technology Officer.

6.2 Any event that appears to satisfy the definition of a serious information security incident must be reported to the ACLS Bureau and ACRO Service Corporation immediately or within 24 hours of the event.

6.3 It is expected that incident reporting, from identification to reporting to the ACLS Bureau, will occur no later than 24 hours.

6.4 Area Agencies on Aging will provide their service providers. vendors and contractors with the ACLS Bureau, AIS IT security reporting policy and coordinate and assist with reporting any observed or suspected security incidents or weakness to the ACLS Bureau.

6.5 All AIS IT information systems and services are required to note and report any observed or suspected security weakness in systems or services.

6.6 All people using the AIS IT information systems shall participate in incident response training provided by the ACLS Bureau as required.

6.7 All people using the AIS IT information systems shall participate in any post-incident activities and follow the required by the ACLS Bureau.

6.8 Falsely reporting AIS security incidents violates this policy.

6.9 All AIS Users must lock down their computers and laptops [CTRL-ALT-delete] when workstations are unattended for any amount of time.

7.0 PASSWORD ACCOUNT MANAGEMENT

Passwords are still the most widely used authentication mechanism for gaining access to information. Strong, unique passwords serve as the frontline of defense against cyber threats. A password must be of sufficient complexity and secrecy that would be impractical for an attacker to guess.

The new password must be different from the old one by at least three characters. That is, you can't change just one or two characters. The new password should be one you have never used before. As a minimum requirement an AIS password must contain at least 8 characters configured from the following categories:

- Uppercase alphabet characters (A–Z)
- Lowercase alphabet characters (a–z)
- Arabic numerals (0–9)
- Non alphanumeric characters (for example ! $ #, %)

POLICY STATEMENT ..... Password Account Management

7.1 Do not allow the use of your AIS account or password by others, including co-workers or family members.

7.2 Create strong passwords consisting of numbers, lower- and upper-case letters. Use a passphrase which is longer and easier to remember.

7.3 Log out and sign off Partner Channel accounts when tasks are completed.

7.4 When AIS activities are active on computer screens, do not leave workstations, devices, or IT Resources unattended without engaging password protections.

7.5 Do not use easily guessed passwords or passphrases, such as “Letmein123#”.

7.6 If you suspect your AIS account has been compromised, please contact the ACLS Bureau support team immediately.

7.7 Do not store AIS password in your browser or allow auto-fill.

7.8 All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set for 10 minutes or less.

7.9 All users must lock down their PCs, laptops, and workstations by locking (control-alt-delete) when the host will be unattended for any amount of time.

8.0 STORAGE OF AIS DATA ON PERSONAL MOBILE DEVICES

To safeguard and protect the confidentiality of AIS client data, the use of personal mobile devices, laptops, tablets and other electronic devices to store AIS data and information is not permitted. In addition to this policy, AIS Users must comply with the applicable SOM Technical Standard 1340.00.110.03 Storage of Sensitive Information on Mobile Devices and Portable Media. *This IT Policy replaces Transmittal Letter 2009-171.*

POLICY STATEMENT .....Storage of AIS Data on Personal Mobile Devices

8.1 The use of personal mobile devices, laptops, tablets and other electronic devices to store AIS data and information is prohibited.

9.0 USE OF PRIVATELY OWNED PORTABLE DEVICES

The use of privately-owned devices presents a special risk to security for IT resources and information. To ensure appropriate security, this policy defines the use of privately owned portable devices to access AIS Partner Channel applications and data.

Portable devices are defined as: any device that can be connected to an information system, computer, or network to provide data storage. Examples of devices include the following:

(i) Laptops, Notebooks, and hybrid devices
(ii) Tablets
(iii) Mobile/cellular phones including smart phones
(iv) Noncompany owned mobile device capable of storing data and connecting to an unmanaged network

In addition to this policy, AIS Users must comply with the applicable SOM Technical Standard 1340.00.020.05 Use of Privately-Owned Portable Devices.

POLICY STATEMENT .....Use of Privately Owned Mobile Devices

9.1 Devices must employ reasonable security measures and manage the location of the devices to prevent unauthorized access.

9.2 Devices must be free from malware infection and run anti-malware protective software.

9.3 The mobile device must not be used to store AIS data.

9.4 The owner of the mobile device understands and agrees that the device may be subject to seizure in the event of a security related incident.

10.0 RECORD MANAGEMENT: DISPOSAL AND RETENTION

There are federal requirements related to retaining data associated with Older Americans Act (OAA) programs. These guidelines aim to ensure compliance, accountability, and the proper delivery of services to older adults. The ACLS Bureau has compiled a Record Retention and Disposal Schedule which addresses records management for OAA information and data.

In addition to this policy, AIS Users must comply with the applicable SOM Technical Standard 1340.00.110.04 Secure Disposal of Installed and Removable Digital Media. *This policy replaces Transmittal Letter 2009-196.*

POLICY STATEMENT ..... Record Management, Disposal, Retention

10.1 Disposal or destruction of AIS records must be done in accordance with the ACLS Bureau Records Retention and Disposal Schedule. See Document 3.

10.2 Ensure that AIS records in the possession of a services provider or vendor are disposed of in accordance with the approved Retention and Disposal Schedule.

10.3 Records that contain personal information must be redacted, burned, pulverized, shredded or otherwise destroyed.

10.4 Electronic records containing personal information must be destroyed or erased so that the information cannot be reconstructed.

10.5 If using media disposal services, Agencies must ensure that these services have adequate security controls in place for the destruction of data.

10.6 Unauthorized removal, modification, or destruction of AIS records is prohibited.

11.0 VENDOR USER ADMINISTRATION

The AIS Vendor User Administration module supports the process for designated AIS Users to create and manage password user accounts to access the NAPIS Online Registration and the secure file retrieval processes. In this role the designated AIS User responsibilities include developing a record system to track users, managing AIS User Profile Applications, creating and disabling accounts, and updating passwords. A Vendor User Administration User Guide can be obtained by contacting the AIS IT staff.

POLICY STATEMENT.....Vendor User Administration

11.1 The Vendor Administrator will manage account access from the initial request for creation to account deactivation.

11.2 The Vendor Administrator will maintain user account documentation of AIS User Profile Applications and history.

11.3 The Vendor Administrator must promptly report changes in duties, agency assignment, or employment status to the ACLS Bureau IT staff and request appropriate user access/account changes.

11.4 The Vendor Administrator will participate in Vendor User Administration training provided by the ACLS Bureau IT staff.

12.0 USER VERIFICATION AUDIT

As part of the statewide compliance for all SOM information technology security standards, the ACLS Bureau has implemented an audit process to review the status of AIS end-user accounts. Using the User Verification Audit, agencies will verify the validity of accounts and access levels for people at their agency who have AIS access rights.

The audit process is completed bi-annually by a designated individual at your agency. Instructions can be obtained by contacting the ACLS Bureau IT staff.

Bi-Annual Review Periods and Due Dates

1st Period	October – March	Due March 31st
2nd Period	April – September	Due September 30th

POLICY STATEMENT..... User Verification Audit

12.1 Designate a person at your agency who will be responsible for completing the bi-annual AIS user verification audit process. This individual should be familiar with AIS applications and user roles.

12.2 The designated person shall verify if the user account is valid and should remain active or should be terminated.

12.3 The designated user shall review the user account AIS access roles for correctness.

12.4 The designated person shall complete the User Verification Audit by the due date.

12.5 The designated user shall appraise the ACLS Bureau if responsibilities change at their agency that impacts their duties as the designated person responsible for completing the User Verification Audit process.

12.6 The agency shall notify the ACLS Bureau if the designated person has left the agency or if a change should be made in this role.

13.0 ELECTRONIC SIGNATURE

The ACLS Bureau uses an electronic signature (e-signature) method for AIS applications and modules to authorize document submission and approval. This policy sets minimum requirements for the use of e-signatures and processes, electronic transactions and electronic records in AIS applications.

In addition to this policy, AIS Users must comply with the applicable SOM Technical Standard 1340.00.080.02 Electronic Signatures. *This policy Replaces Transmittal Letter 2009-194.*

POLICY STATEMENT..... Electronic Signature

13.1 Agencies must maintain an internal record of people authorized to process e-signatures in AIS modules.

13.2 By completing the e-signature process in AIS applications, the agency-official agrees to the validity of the individual providing their e-signature and submission of the document and data to the ACLS Bureau.

13.3 An e-signature is not valid if the individual does not have signature authority to sign the record approving the transaction.

13.4 All AIS Users, business or vendor partners have approved AIS User Profile Applications file authorizing access to the AIS Partner Channel.

13.5 All e-signature submissions must be unique and unduplicated.

14.0 AIS USER ROLES AND TRAINING

The AIS User Profile Applications must be completed before access is granted to Partner Channel applications. AIS Users are assigned different levels of authority based on their job duties and assignments. The completed form must be signed by the user's immediate supervisor or an appropriate party at their agency. Submit the completed form to your ACLS Bureau program coordinator or AIS IT staff.

The AIS User Profile Applications can be found under the link *AIS Forms and Resources* on the Business Site.

14.1 AIS User Roles

User roles and permissions play a pivotal role by defining and controlling access levels for different users within AIS applications. A user role represents a specific set of tasks or responsibilities an assigned user can perform. The AIS User Profile Application outlines some of the basic user role-based permissions. Listed below are descriptions of relevant end-user access levels and their function. For more information on AIS user roles, see your program coordinator or the ACLS Bureau IT staff.

AIS User Role	Function	AIS Application
Data Entry	Able to enter data and make edits. May save a process as complete for Data Admin approval.	• AMPS • MATF • VAFA • PREVNT • SCSEP
Data Admin	Able to review, approve, affix electronic signature and submit to ACLS Bureau for processing.	• VPAG • Cash Request • OAA • FSR • AAA Assessment Guide
AIP/MYP Viewer	Can only view and download the 'AIP/MYP document' files uploaded by the ACLS Bureau Administrator	Annual and Multi-Year Implementation Plan (AMPS)
Above are general user access roles and a brief list of associated applications. There is an array of functionality and permissions that varies across applications for a user role.		

14.2 AIS Training

Because most data security breaches involve human error, security awareness training can reduce this risk. Sections 4.0-9.0, and 15.0 of this Guide reinforce basic IT security awareness training principles.

The ACLS Bureau IT staff provides security awareness training, technical support, and end-user training for AIS applications. Agencies must oversee the implementation of

security awareness training within their agency. For training guides or training sessions on AIS modules, contact the ACLS Bureau IT staff.

In addition to this policy, AIS Users must comply with the applicable SOM Technical Standard 1340.00.030.01 Security Awareness and Training. *This IT policy replaces Transmittal Letter 2007-148.*

POLICY STATEMENT ..... AIS User Roles and Training

14.1 AIS Users shall participate in AIS Partner Channel onboarding training as required.

14.2 AIS Users shall participate in security awareness information and training provided by AIS IT staff as required.

14.3 Agencies that manage SOM AIS information and data must ensure that AIS Users receive security training.

14.4 The Agency IT Security Officer or other appropriate staff should work with the ACLS Bureau IT staff to meet security training needs.

15.0 AGENCY IT SECURITY OFFICER

To ensure the security of AIS data, Area Agencies on Aging and other AIS network entities should have a designated IT security officer. The individual responsible for IT security at your agency is an integral part of AIS security and risk management. The IT security officer maintains that appropriate operational security controls are in place to meet state and federal law, regulations, and policies for SOM information. The Agency IT Security Officer serves as the primary liaison between agency staff and AIS management staff. Duties of the Agency Security Officer include but are not limited to the following:

I. Assist the Agency in ensuring that information technology systems have adequate security controls in place to meet all state and federal laws and regulations.

II. Ensure that internal agency policies and procedures are implemented, maintained, and enforced to protect AIS data.

III. Assists Agency managers in establishing a tracking and reporting strategy for AIS information security matters.

IV. Assist Agency managers in establishing general information technology security awareness programs and training.

V. Understands that the SOM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

VI. Keep malware and virus definitions up to date so that the latest versions of attacks can be detected.

POLICY STATEMENT.....Agency Security Officer

15.1 Ensure that adequate information technology security controls are in place to meet all state and federal laws and regulations to protect AIS data and information.

15.2 Review and respond to security notifications from the ACLS Bureau regarding AIS information systems.

15.3 Develop a remote work plan for IT equipment that will be used by AIS Users working remotely.

15.4 Ensure that a business continuity plan that considers information security requirements shall be implemented and tested at least once per calendar year.

15.5 The Agency IT Security Officer should take the lead in implementing and management of disaster recovery planning and emergency preparedness procedures at their agency.

16.0 EMERGENCY PREPARDNESS AND DISASTER RECOVERY

Having a disaster recovery plan is essential to ensure the best corrective response to incidents such as natural disasters, man-made incidents, cybercrime, fire, and sabotage. To ensure that federal and state reporting requirements of Older Americans Act data is met, Area Agencies on Aging must develop and implement IT Disaster Recovery Plans to protect AIS program data and ensure business continuity.

Your agency's IT Disaster Recovery Plan should include strategies, procedures, and protocols to help recover the AIS IT infrastructure and systems after a disruptive event. Further, it should include steps to restore AIS data and resume normal business operations.

POLICY STATEMENT..... Disaster Recovery Plan

16.1 Agency management must ensure information security, continuity of operations, and an IT disaster recovery plan is part of their agency's processes and procedures.

16.2 Agency management must inform the ACLS Bureau of any event that disrupts the flow of AIS data.

16.3 Agency management must ensure that business partners who provide AIS data to the SOM are responsible for maintaining a Disaster Recovery Plan.

16.4 Assist staff with understanding and implementing continuity of operations and IT Disaster Recovery policies, standards, and procedures.

16.5 Prioritize your most critical AIS operations so your recovery efforts focus on restoring those operations first.

16.6 The Agency IT Security Officer should take the lead on implementing and management of disaster recovery planning and emergency preparedness procedures at their agency.

16.7 Disaster Recovery Plans should be tested frequently and updated annually or when there is a need for change.

17.0 ACKNOWLEDGMENT OF RECEIPT

Acknowledging receipt of this guide is managed electronically. When logging into the AIS Partner Channel you will be required to acknowledge receipt of the *Aging Information System Information Technology Security Guide*. This acknowledgement indicates that you have read and understand the policies, procedures, and best practices, and agree to comply with all policies and procedures contained in this Guide.

Further, it is expected that Area Agency on Aging Directors/Chief Information Officers, Senior Volunteer Program Directors, and Grant Program Managers agree to disseminate this Guide to staff, service program providers, and vendors affiliated with their agency who access the AIS Partner Channel.

18.0 BEST PRACTICES

AIS Users are responsible for exercising good judgment and best practices to safeguard the security and quality of AIS data. The AIS end-user is the best line of defense against cyber threats. AIS data is important and tells the story of past, present, and most importantly, the future needs of OAA services supporting Michigan's older adult population.

18.1 Use password-protected screensaver with automatic shut-down set for less than 10 minutes for all PCs, laptops, and workstations.

18.2 When working with AIS data, lock the screen (CTRL-ALT-delete) when away from your computer.

18.3 **Shut down your computers properly and often**. It's common to keep computers running throughout the work week but shutting them down is essential for the health and security of the equipment. Most software updates require you to restart your computer to run successfully, so shutting down equipment is necessary for regular software maintenance.

18.4 **Don't disable built-in protections**. Use an antivirus to conduct automatic and manual scans of files on your device.

18.5 When working remotely, adjust your Wi-Fi settings. Modify your router's default password, adjust default settings, and reduce signal strength to make them more secure. Have a dedicated, secure place that is safe from virtual and physical break-in.

18.6 Notify your agency security staff and the ACLS Bureau IT Staff if you detect any suspicious activity.

18.7 Secure portable devices in the office and while traveling.

18.8 **Keep Antivirus Software Enabled and Updated.** No operating system is immune to viruses and other malware. Unfortunately, though, Windows users are targeted disproportionately more than macOS and Linux users. If you are a Windows user, then you need to keep antivirus software enabled and always updated.

18.9 **Properly discard information.** When disposing documents and files shred and discard in accordance with the Records Retention and Disposal Schedule.

18.10 Don't have sensitive work conversations near home smart devices.

18.11 Don't use public Wi-Fi, e.g., coffee shops, airports, etc.

18.12 Don't leave sensitive information exposed physically or online.

18.13 Be aware of phishing scams.

18.14 Participate in IT awareness training offered by your agency.

DOCUMENTS

Document 1 ..... AIS Incident Report Form

Document 2 ..... AIS User Profile Application

Document 3 ..... Records Retention and Disposal Schedule

Document 4 ..... AIS Network Diagram

ACRONYMS

AAA .....Area Agency on Aging

ACLS Bureau .....Bureau of Aging, Community Living, and Supports

AIS ..... Aging Information System

AMPS ..... Annual and Multi Year Planning System

FSR .....Financial Summary Report

IT .....Information Technology

MAYF .....Meri Award Trust Fund

NAPIS .....National Aging Program Information System

NIST .....National Institute of Standards and Technology

OAA ..... Older Americans Act

PREVNT.....Prevent Elder and Vulnerable Adult Abuse, Exploitation Neglect Today

SCSEP..... Senior Community Service Employment Program

SOM .....State of Michigan

SUA ..... State Unit on Aging

VAFA ..... Volunteer Annual Funding Agreement

VPAG ..... Volunteer Program Assessment Guide

TERMS AND DEFINITIONS

AIS Network
The AIS Network comprises several bodies (federal, state, service providers, local partnerships) that work together to provide services and supports to Michigan's adult population.

Area Agency on Aging
Michigan has 16 Area Agencies on Aging (AAA) mandated by the Older Americans Act. AAAs serve as local entities who oversee the comprehensive service system for the delivery of social, nutrition, and long-term services and support to older adults. The AAAs either oversee this system directly or they contract with local service providers.

AIS Data and Information
AIS data and information include information derived from client registration/intake forms, system generated reports, printed materials, electronic import files,

Authorized User
An individual or automated application or process that is authorized to access the resource by the system owner, in accordance with the system owner's procedures and rules.

ACLS Bureau AIS IT Support Staff
For information and technical support with AIS applications contact the AIS IT staff at MDHHS-AIS-Security@michigan.gov.

Cybersecurity Incident
Cybersecurity Incident is a violation (breach) or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

Data Use Agreement
A Data Use Agreement is a formal, legally binding contract that outlines the terms and conditions for the use and protection of data, particularly sensitive or confidential information. It includes provisions for data governance, confidentiality, security measures, and liability.

Data Sharing Agreement
A Data Sharing Agreement may not have the same level of detail regarding data protection as a Data Use Agreement and may focus more on the sharing of data rather than its use. While both agreements are related to data handling, the DUA is more focused on the use and protection of data, whereas a Data Sharing Agreement may cover broader aspects of data sharing.

Data Protection
Data protection is the process of safeguarding important information from corruption, compromise, or loss. The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates. There is also little tolerance for downtime, which can make it impossible to access important information.

Data Security
Data Security refers to the measures taken to protect data from unauthorized access or cyber threats. Security measures are designed to prevent unauthorized individuals from accessing, altering, or stealing data. This might involve technical measures like encryption and multi-factor authentication or organizational measures like access control policies and employee training.

Disaster Recovery Plan
A disaster recovery plan is a set of actions that help an organization recover its technology and operations following a significant impacting event.

End-User
A person who interacts with the system usually possesses a unique identifier (like a username) and authentication credentials (such as a password).

Older Americans Act
Authorized in 1965, the Older Americans Act is a federal law that funds a network of community-based programs and services to help older adults maintain their independence and well-being in their communities. provides grants to states and local areas for services like nutrition assistance, senior centers, in-home care, transportation, elder abuse prevention, and caregiver support, primarily for individuals aged 60 and older.

Older Michiganians Act
The Older Michiganians Act (1981 PA 180) created the Commission on Services to the Aging within the Executive Office of the Governor to oversee Michigan's implementation of the Older Americans Act of 1965. The Public Act created the Office of Services to the Aging (State Unit on Aging) to authorize the designation of Area Agencies on Aging and established programs and services to support Michigan's adult population.

Password Phrase
A strong passphrase should generally contain 15 characters, with a mixture of uppercase and lowercase letters, numbers, and symbols. The phrase shouldn't be based on a popular expression but a sequence of random words that are not logically connected so that they can't be guessed.

Service Program Provider
A person (vendor, contractor, third party, etc.) or entity that has contracted or signed an agreement with the SOM to perform a service or provide a product in exchange for valuable consideration

State Unit on Aging (SUA)
The Older Americans Act Established State Units on Aging to serve as the state agency responsible for planning and policy development of Older Americans Act activities. The ACLS Bureau is Michigan's designated SUA.

Sensitive Data
Sensitive data is any kind of information protected against unwarranted disclosure. It involves a wide range of categories, including personal data, financial information, proprietary details, health records, or trade secrets. Sensitive data collected in several

AIS modules include name, address, phone number, date of birth, and financial transactions.

Security Incident
A single or series of unwanted or unexpected Security Events that compromise business operations with an impact on Information Security.

Transmittal Letter
Transmittal Letters are directives issued by the ACLS Bureau that provide official policy guidance, procedural changes, and programmatic information. Transmittal Letters are issued to Area Agencies on Aging, grant agencies, and the Aging Network.

User Role
User roles categorize users based on their job functions, such as Data Entry, Data Administrator, or Viewer. Each role has specific permissions that dictate what actions a user can perform, such as creating content, modifying settings, or viewing information.

REVISION HISTORY

This table contains a history of this publication's revisions.

Version	Summary of Change	Date Updated	Updated By
1.0	Original	10/01/2025	ejb

Notes