	No: Information Technology **IT-14**
# State of Ohio Administrative Policy	**Effective:** December 21, 2018
Data Encryption and Securing Sensitive Data	**Issued By:** Robert Blair, Director

1.0   Purpose

This policy in conjunction with Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography," provides guidance to agencies as they take steps to protect *sensitive data* and *information*.

A glossary of terms found in this policy is located in Appendix A - Definitions. The first occurrence of a defined term is in ***bold italics***.

2.0   Policy

Increased connectivity and mobility makes more data available to individuals, businesses and agencies. Consequently, sensitive information is more vulnerable to unauthorized disclosure, modification or destruction. Therefore, it is critical that state agencies implement the appropriate safeguards to protect sensitive data and information. This policy outlines the requirements for identifying and securing sensitive data as well as the devices and *media* on which sensitive data resides.

2.1   **Identify and Label Sensitive Data:** To help ensure that all sensitive data is protected, state agencies shall classify data, systems, media, devices and electronic transmissions. Agencies shall establish procedures to identify, label and secure data in accordance with Ohio Administrative Policy IT-13, "Data Classification."

2.2   **Use Only State-Approved Strong *Encryption*:** Any use of encryption to protect sensitive data shall conform to Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography."

2.2.1   Agencies shall ensure that a cryptographic key management plan is in place that protects the creation, distribution and storage of cryptographic keys as described by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57, Recommendations for Key Management Parts 1, 2 and 3.

The Ohio Department of Administrative Services

Office of Information Technology | 30 East Broad Street, 39th Floor | Columbus, Ohio 43215 | 614.644.6446 | State.CIO@das.ohio.gov   Spencer Wood, Interim Assistant Director/State CIO

2.3 **Secure Sensitive Data in Transmission:** Agencies shall secure sensitive data in transmission. Whenever sensitive data travels over the Internet or other untrusted channels, as a minimum, encryption shall be used to safeguard the data.

   2.3.1 In particular, the following forms of transmission over untrusted channels shall be encrypted:

   - e-mail,
   - pages on state-controlled Web sites, instant messaging,
   - remote printing,
   - data transfers,
   - copying of data to removable media, and
   - any wireless transmission.

   2.3.2 Agencies shall establish a process to check data in transmission for activities that risk unauthorized access to or disclosure of sensitive data. There are different means of checking for these types of activities and they include increased activity logging, spot audits, the use of content monitoring and lexical analysis tools among others.

2.4 **Secure Sensitive Data at Rest:** State agencies shall secure sensitive data at rest. Regardless of whether access is via trusted or untrusted channels, state agencies shall provide strong access controls for sensitive data at rest. As a minimum, agencies shall protect sensitive data at rest through encryption.

   2.4.1 The following agency practices shall be in place to secure access to sensitive data systems:

   2.4.1.1 Implement restrictions on the downloading of sensitive data;

   2.4.1.2 Apply authorization controls so that individual access is limited to a need-to-know basis based on the *user*'s role in the state agency;

   2.4.1.3 Employ a session lock for accounts, including those initiated via remote access or *portable devices*, that requires reauthentication after 30 minutes or less of inactivity;

   2.4.1.4 Implement a process for prompt deactivation of accounts for users who are no longer employed, shall no longer have access, or are subject to an action requiring deactivation; and

   2.4.1.5 Conduct a regular validation of user accounts to ensure that access rights are assigned, as appropriate.

2.5 **Secure Backups:** In performing sensitive data backups and restorations, state agencies shall ensure:

   2.5.1 Encryption is consistently applied to backup devices, media and active data.

2.5.2   Data backups enforce the most current access controls.

2.5.3   Reuse of backup media is limited to the same set of sensitive data or is securely sanitized in accordance with NIST SP 800-88, "Guidelines for Media Sanitization," if it is used for another purpose.

2.5.4   Backup media is destroyed in accordance with NIST SP 800-88 guidelines once it is no longer necessary.

2.5.5   Appropriate physical security controls shall be in place, including:

   2.5.5.1   Physical access to backups of sensitive data shall be limited to authorized personnel only.

   2.5.5.2   Physical transportation of backup media shall be secure.

       2.5.5.2.1   Transport shall be provided by a state employee or state-approved secure carrier.

       2.5.5.2.2   When possible, backup media shall be transported using a locked, tamper-proof box to secure the media.

   2.5.5.3   Physical storage of sensitive data backups and restorations shall be located at a state-owned or state-approved, secure facility.

2.6   **Secure Sensitive Data on Portable Devices and Media:** As a minimum, agencies shall implement the following controls for the placement of sensitive data on portable devices and media:

2.6.1   A procedure shall be developed for authorizing the placement of sensitive data onto portable devices and media. The procedure shall include the following:

   2.6.1.1   A required risk assessment that will assist in determining the level of risk associated with the use of a given device or type of media.

   2.6.1.2   Written authorization for the placement of sensitive data on portable devices and media.

   2.6.1.3   Written acknowledgement from each user that he/she agrees to comply with the security requirements of this policy, state IT security policies and agency IT security policies.

2.6.2   The use of encryption and strong passwords shall be used to protect sensitive data on portable devices and media. Encryption may be employed at the data level, file level, or operating system.

2.6.3 A procedure shall be developed for the removal or destruction of sensitive data on portable devices and media that aligns with NIST SP 800-88 and the requirements outlined in Ohio Administrative Policy IT-05, "Disposal, Servicing and Transfer of IT Equipment."

2.6.4 Agencies shall prohibit the placement of sensitive data on portable, non-state devices.

2.7 **Physically Secure Sensitive Data:** State agencies shall secure the physical devices, locations and facilities used for sensitive data processing and storage.

2.7.1 Only authorized personnel shall be allowed to access or remove devices and media containing sensitive data.

2.7.2 In no event shall unencrypted sensitive data be stored or transported in a manner that is not physically secure. For unencrypted sensitive data, "physically secure" means implementing multiple layers of physical security that use facilities and services designed for securing high-risk data and certifying that the facilities or services take the necessary physical security precautions.

2.8 **Communicate Expectations for Handling Sensitive Data:** Agencies shall ensure that users are aware of all of the requirements associated with the protection of sensitive data and that they actively acknowledge their role. Agencies shall require users to agree in writing to take precautions to protect sensitive data. The written agreement shall include the following:

2.8.1 Everyone has a duty to protect sensitive data;

2.8.2 Sensitive data shall not be disclosed without authorization;

2.8.3 Access to sensitive data shall not be provided without proper authorization;

2.8.4 Sensitive data shall not be stored on devices that are personally-owned or otherwise not controlled by the state;

2.8.5 There is no expectation of privacy when using state devices. The state has the right to access, inspect and monitor any state device or service including any files on or communications through state devices or services;

2.8.6 In support of an investigation, the state may gain access to, or take custody of, non-state devices or services upon which the user has or appears to have placed state data; and

2.8.7 Contain the penalties associated with violating the agreement.

2.9 **Be Prepared to Respond to a Security Incident:** Agencies shall develop incident response procedures that specifically address a compromise or exposure of sensitive data.

2.9.1 Agency incident response procedures shall include a plan to notify and respond to persons affected by the security incident.

2.9.1.1 Note that Section 1347.12 of the Ohio Revised Code states that an agency may not need to initiate the plan to notify persons affected by a security incident if the compromised sensitive data is protected by encryption.

2.9.2 There are risks and costs associated with the compromise of sensitive data that extend beyond the costs of identity theft protection to those affected, or the steps taken to detect and recover from a security incident. There may also be fines, negative publicity, or loss of public trust involved. Each agency's incident response capability shall incorporate efforts to mitigate these greater risks and costs.

2.10 **Exception Process**: To request an exception to one or more of the requirements outlined in this policy, please complete an IT Security Exception Request form.

2.10.1 The form is located within the IT Enterprise Services Portal under the "Services & Products" category.

2.10.2 If you have any questions, please contact DAS OISP (refer to Section 5.0 Inquiries for contact information).

2.11 **Implementation**: Due to the length of time that this policy has been in effect, it is expected that agencies are already in alignment with data encryption and securing sensitive data requirements. For compliance related questions, please contact DAS OISP (refer to section 5.0 Inquiries for DAS OISP contact information).

3.0 Authority

ORC 125.18, 1347.12

4.0 Revision History

Date	Description of Change
07/25/2007	Original policy.
07/01/2015	Converted Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data," into an Ohio Administrative Policy. Ohio IT Bulletin ITB-2007.02 is now Ohio Administrative Policy IT-14. Added requirements to ensure alignment with NIST special publications related to key management and media sanitization. Included new physical security requirements related to the transportation of backup media. Added a reference to the new Ohio Administrative Policy IT-13, "Data Classification".
12/21/2018	Minor updates made to align with current terminology and security practices.
12/21/2019	Scheduled policy review.

5.0   Inquiries

Direct inquiries regarding this policy to:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 19th Floor
Columbus, Ohio 43215

614.644.9391| state.isp@das.ohio.gov

State of Ohio Administrative Policies may be found online at:
www.das.ohio.gov/forStateAgencies/Policies.aspx

Additional information regarding the Office of Information Security & Privacy may be found online at infosec.ohio.gov.

Appendix A - Definitions

a. Encryption. The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

b. Information. Data processed into a form that has meaning and value to the recipient to support an action or decision. "Information" is often used interchangeably with "data" in common usage and in this policy.

c. Media. Any device that is capable of storing information. Media is not required to be capable of processing information.

This definition includes, but is not limited to, the following:

- Diskettes
- External/removable hard drives
- Flash memory (e.g., secure digital (SD), Compact Flash, secure digital high-capacity (SDHC), solid state drives, memory sticks)
- Magnetic tapes
- Portable Devices
- Optical media such as compact disks (CDs), digital video disks (DVDs), etc.
- Thumb drives (USB keys)/jump drives

d. Personally Identifiable Information (PII). "Personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,

- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

e. <u>Portable Devices</u>. Computer or device designed for mobile use. For the purposes of this policy, a portable device includes laptops, smartphones or tablets.

f. <u>Sensitive Data</u>. Sensitive data is any type of computerized data that presents a high or moderate degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of ***personally identifiable information*** that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, and Criminal Justice Information under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

g. <u>User</u>. An individual or (system) process authorized to access an information system.[1]

Appendix B - Resources

Document Name
NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations   http://csrc.nist.gov/publications/PubsSPs.html
NIST Special Publication 800-57, Recommendations for Key Management Parts 1, 2 and 3   http://csrc.nist.gov/publications/PubsSPs.html
NIST Special Publication 800-88, Guidelines for Media Sanitization   http://csrc.nist.gov/publications/PubsSPs.html
Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography"   http://www.das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx
Ohio Administrative Policy IT-05, "Disposal, Servicing and Transfer of IT Equipment"   http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies.aspx
Ohio Administrative Policy IT-13, "Data Classification"   http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies.aspx
Ohio Revised Code Section 1347.12   http://codes.ohio.gov/orc/1347.12

---

[1] "FIPS 200, Minimum Security Requirements for Federal Information and Information Systems." U.S. Department of Commerce National Institute of Standards and Technology, March 2006. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>.