Standard PR.AC: Encryption of Computing Devices and Information

February 11, 2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

Approval

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.11 12:41:00 -05'00'

Steven Hernandez _____ **Date**

Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	12/31/2018	Initial draft
1.1	2/9/2020	Underwent annual policy review for accuracy and timeliness and to incorporate updates to NIST SP 800-53 Rev. 4. No updates were required as of December 2019. Updated external email communications using PIV card.
1.2	1/15/2021	Annual review for accuracy and timeliness. Updated section 2.1.2 to reference Department Password Standard. Updated policy exception verbiage.

Table of Contents

1. INTRODUCTION

1.1. Purpose

This document falls within the Instruction Protect and establishes the Department Standard for the encryption of computing devices and information. In doing so, it supersedes any prior documentation establishing such standards.

1.2. Scope

The standards established in this document apply to all employees, contractors, and users authorized to access ED information systems, systems operated or maintained on behalf of ED, or ED information.

2. STANDARDS

2.1. Data Encryption

All sensitive information (i.e., data) must be encrypted when at rest and in transit.

2.1.1. Data at Rest

Sensitive data stored either on GFE or non-GFE (contractor-owned) equipment must be safeguarded in accordance with National Institute of Standards and Technology (NIST) guidance and OCIO Policy, including but not limited to the following standards:

a) Folders/files containing sensitive PII or other sensitive data stored in a shared drive must be encrypted and the folders configured to restrict access on a need-to-know basis.

b) Data backups must be encrypted and securely transported/filed/archived.

c) Cryptographic mechanisms must be employed to protect the integrity of audit information related to high-value assets (e.g. log, and audit tools).

2.1.2. Data in Transit

a) When accessed via remote access, sensitive information must be protected with end-to-end encryption.

b) Email and attachments that contain sensitive information must be encrypted using the user's Personal Identity Verification (PIV) card to external recipients. Internal email communications are TLS 1.2 enforced and meet the requirements of this standard.

c) When the capability of encrypting sensitive data for external distribution using a PIV card is not available, communication must be encrypted using a FIPS 140-2 compliant version

of WinZip.

a) Password protected files shall comply with the Department's password standard, as define in *Standard PR.AC: Password Parameters*.

2.2. Public Key Infrastructure (PKI) Use

a) Public key certificates used by the Department must be issued in accordancewith Federal PKI policy.

b) Public key certificates used by the Department must be validated to the Federal PKI trust anchor for all uses, including but not limited to encryption, authentication, and authorization applications.

c) Digital signature capabilities must be validated to the Federal PKI trust anchorand implemented in accordance with Federal PKI policy and NIST standards and guidelines.

d) For employees and contractors, the Department must use PIV credentials to validate digital signatures.

e) For individuals that fall outside the scope of PIV applicability, the Department must leverage approved Federal PKI credentials to validate digitalsignatures.

f) All devices containing sensitive information must use a key recovery mechanism so that authorized personnel with legitimate need can access encrypted information.

g) Use of encryption keys which are not recoverable by authorized personnel is prohibited.

h) A non-owner of an encryption key may request to recover the key, however such requests must be explicitly authorized by the ED Chief Information Security Officer (CISO).

2.3. Device Encryption

a) Servers that authenticate, store, process, and/or transmit sensitive informationmust be encrypted.

b) If server encryption is not technically feasible, all folders and/or filescontaining sensitive information must be encrypted.

c) The implemented level of encryption must be sufficient to mitigate the risk severity. For example, a server storing highly sensitive information, such as payroll data, whole disk encryption would not be sufficient to protect information at rest. Files and folders should also be encrypted.

d) Whole disk encryption or container encryption must be employed on all desktops, laptops and mobile/portable devices.

e) No sensitive data can be stored at any time on unencrypted GFE or non-GFE.

f) All storage media (hard drives, USB drives, CDs, etc.) must be encrypted to meet the minimum standards for encryption of FIPS 140-2.

g) Legacy devices that do not employ encryption capabilities (e.g., magnetic media, backup tapes, hard drives, or floppy disks) are not be allowed to store sensitive information unless they are secured in Principal Office-defined, controlled environments.

h) All photocopiers, printers, fax machines, and multifunctional machines that have storage data transmission capability must be encrypted.

i) Personally-owned mobile telephones, tablets, and other smart and storage devices must not be used to store and access government sensitive information, unless granted a written exception from the ED CISO and managed by an approved enterprise mobile device management (MDM) solution and encryption mechanism. The MDM solution must be configured to the most restrictive settings practicable and allow for remote wipe in the event of an incident involving ED data.

2.4. Websites and Web Services

a) All Department Websites and Web services must employ secure connections, such as Hypertext Transfer Protocol Secure (HTTPS) and HTTP Strict Transport Security (HSTS).

b) Use of a Social Security number as an identifier—even if masked—is prohibited on all existing and new ED websites.

c) POs must use the most current Transport Layer Security (TLS) version. TLS must be implemented and configured in accordance with the recommendation of NIST SP 800-52 as amended.

d) All Department second-level .gov domains will be preloaded to enforce the use of HTTPS where applicable. Second-level .gov domains that are only used to redirect visitors to other Websites and are not used on intranets are excellent preloading candidates.

e) Allowing HTTP connections for the sole purpose of redirecting clients to HTTPS connections is acceptable and encouraged. HSTS headers must specify a max-age of at least 31536000.

f) All Department Websites and Web services must remove support for known-weak cryptographic protocols and ciphers, including:
    i. Protocols
        i. SSLv2 and SSLv3 must be disabled on Web servers
    ii. Ciphers
        i. 3DES and RC4 ciphers must be disabled on Web servers

2.5. Email Server Security

The following protocols must be used to secure email transmissions.

a) All Internet-facing email servers must use STARTTLS.
b) All second-level agency domains must have valid SPF/DMARC records, with a policy of "reject" for second-level domains and mail-sending hosts.
c) Secure Sockets Layer (SSL)v2 and SSLv3 must be disabled on email servers.
d) 3DES and RC4 ciphers must be disabled on email servers.

3. RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

APPENDIX A: ACRONYMS

ACS	Administrative Communications System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSO	Computer Security Officer
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
IAS	Information Assurance Services
ISO	Information System Owner
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PO	Principle Office
SP	Special Publication
U.S.C	United States Code
VPN	Virtual Private Network

APPENDIX B: GLOSSARY

Term	Definition	Source
Advanced Encryption Standard (AES)	An approved algorithm for encryption. Its implementation and use must conform to FIPS 197.	NIST SP 800-175B, page 13
Algorithm	A well-defined computational procedure that takes variable inputs, including a cryptographic key (if applicable), and produces an output.	NIST SP 800-175A Cryptographic algorithm, page 1
Authentication	A process that provides assurance of the source and integrity of information that is communicated or stored, or that provides assurance of an entity's identity.	NIST SP 800-175A
Backup	The process of copying information or processing status to a redundant system, service, device or medium that can provide the needed processing capability when needed.	NIST SP 800-152 Backup
Certificate (or public key certificate)	A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity identified in the certificate. Additional information in the certificate could specify how it is used and the validity period of the certificate.	NIST SP 800-175B, page 3

Term	Definition	Source
Compensating control	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.	NIST SP 800-37, rev1 *Compensating Security Controls*
Confidentiality	The property that sensitive information is not disclosed to unauthorized entities	NIST SP 800-175A
Container	The file used by a virtual disk encryption technology to encompass and protect other files.	NIST SP 800-111
Cryptography	The science of information hiding and verification. It includes the protocols, algorithms and methodologies to securely and consistently prevent unauthorized access to sensitive information and enable verifiability of the information. The main goals include confidentiality, integrity authentication and source authentication.	NIST SP 800-175A
Decryption	The process of changing ciphertext into plaintext using a cryptographic algorithm and key.	NIST SP 800-175B

Term	Definition	Source
Digital signature	The result of a cryptographic transformation of data that, when properly implemented with a supporting infrastructure and policy, provides the services of: 4. Origin (i.e., source) authentication; 5. Data integrity authentication; and, 6. Support for signer non-repudiation.	NIST SP 800-57 part1, rev4, page 5
Encryption	The process of transforming plaintext into ciphertext using a cryptographic algorithm and key for the purpose of security or privacy.	NIST SP 800-175A NIST SP 800-57, part1, rev4
Encryption key	A key used to encrypt and decrypt information other than keys. Key-encryption key is a cryptographic key that is used for the encryption or decryption of other keys.	NIST SP 800-57, part1, rev4 Data-encryption key
End-to-end encryption	Encryption from the individual requesters to the Web service interface and from the Web service interface to the legacy backend system. This is done to ensure that sensitive data are not exposed in transit over external and internal networks.	NIST SP 800-95

Term	Definition	Source
Federal Information Processing Standard (FIPS) 140-2 validated	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP).	NIST SP 800-53, rev4, FIPS-Validated Cryptography
Federal Public Key Infrastructure (PKI) trust anchor	The trust anchor refers to the Federal PKI root certificate operated by the Federal PKI Management Authority. This root certificate is the trusted source of all Federal PKI certificates. For additional information, refer to https://www.idmanagement.gov and Federal PKI policy.	NIST SP 800-175A, page 20 footnote20
File Encryption	The process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided.	NIST SP 800-111

Term	Definition	Source
High-Value Asset	The Federal Government's most critical and high impact information and information systems and the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	NIST SP 800-175A; BOD 18-02
Hypertext Transfer Protocol Secure (HTTPS)	A protocol that is defined as HTTP over Secure Sockets Layer (SSL)/TLS. HTTPS supports authentication, confidentiality, and integrity of data sent between the endpoints.	NIST SP 800-95
Hypertext Transfer Protocol (HTTP) Strict Transport Security (HSTS)	A simple and widely supported standard to protect visitors by ensuring that their browsers always connect to a Website over HTTPS. HSTS exists to remove the need for the common, insecure practice of redirecting users from http:// to https:// Uniform Resource Locators (URLs).	https://https.cio.gov/hsts/
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	NIST SP 800-53, rev4

Term	Definition	Source
Information at rest	The state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies.	NIST SP 800-53, rev4, SC- 28
Information in transit	When information is transmitted over a network.	NIST SP 800-175A
Integrity	The property that protected data has not been modified or deleted in an unauthorized and undetected manner.	NIST SP 800-175A

Term	Definition	Source
Key	A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce, reverse or verify the operation, while an entity without knowledge of the key cannot. Examples include: • The transformation of plaintext data into ciphertext data; • The transformation of ciphertext data into plaintext data; • The computation of a digital signature from data; • The verification of a digital signature on data; • The computation of an authentication code from data; • The verification of an authentication code from data and a received authentication code; and • The computation n of a shared secret that is used to derive keying material.	NIST SP 800-57, rev4 Cryptographic key (key)
Key management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., counters) during the entire life cycle of the keys, including the generation, storage, establishment, entry and output, and destruction.	NIST SP 800-175A

Term	Definition	Source
Media	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.	NIST SP 800-53, rev4
Mobile device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and, (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers	NIST SP 800-79-2
Mobile device management (MDM)	Mobile enterprise security technology used to address security requirements.	NIST SP 800-163, page 9

Term	Definition	Source
Personal Identity Verification (PIV) card	The physical artifact (e.g., identity card, "smart" card) issued to an applicant by an issuer that contains stored identity markers or credentials (e.g., a photograph, cryptographic keys, digitized fingerprint representations) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).	NIST SP 800-79-2
Personally identifiable information (PII)	Any information about an individual maintained by an agency, including: (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and, (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.	NIST SP 800-122
Personally-owned devices	A non-organization-controlled device owned by Personnel, over which the organization have no direct supervision and authority over the device of required security controls or the assessment of control effectiveness.	NIST SP 800-46, rev 2, Bring Your Own Device (BYOD) NIST SP 800-53rev4, AC- 20

Term	Definition	Source
Public Key Infrastructure (PKI)	The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.	NIST SP 800-53, rev4
Remote access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., Internet).	NIST SP 800-53, rev4
Sensitive information	Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act); that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.	NIST SP 800-53, rev4

Term	Definition	Source
Transport Layer Security (TLS)	A protocol created to provide authentication, confidentiality, and data integrity between two communicating applications. Used to protect sensitive data during electronic dissemination across the Internet.	NIST SP 800-52, rev 1, page vi
Whole disk encryption	The process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product.	NIST SP 800-111

APPENDIX C: RESOURCES AND REFERENCES

- NIST Special Publication (SP) 800-53, (as amended): *Security and Privacy Controls for Federal Information Systems and Organizations*
- Federal Information Security Modernization Act of 2014 (FISMA 2014)