Asset Management Practices, version 1.0.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document Owner: Information Security Committee
Last Review Date: February 2018

Asset Management Practices

Purpose

The purpose of the SPPS Asset Management Practices is to establish the rules for the control of hardware, software, applications, and information used by SPPS.

Audience

The SPPS Asset Management Practices applies to individuals who are responsible for the use, purchase, implementation, and/or maintenance of SPPS Information Resources.

Contents

- Hardware, Software, Applications, and Data
- Mobile Devices
- Media Destruction & Re-Use
- Backup
- Removable Media

Practices

Hardware, Software, Applications, and Data

- All hardware, software and applications must be approved and purchased by SPPS Technology Services.
- Installation of new hardware or software, or modifications made to existing hardware or software must follow approved SPPS procedures and change control processes.
- All purchases must follow the defined SPPS Purchasing Standard.
- Software used by SPPS employees, contractors and/or other approved third-parties working on behalf of SPPS must have valid software licenses.
- Software installed on SPPS computing equipment, outside of that noted in the SPPS Standard Software List, must be approved by Technology Services Management and installed by SPPS Technology Services personnel.
- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential** or **internal information**.
- The use of **cloud computing applications** must be done in compliance with all laws and regulations concerning the information involved, e.g. personally identifiable information (PII), protected health information (PHI), corporate financial data, etc.
- Two-factor authentication is recommended for external **cloud computing applications** with access to any **confidential information** for which SPPS has a custodial responsibility.
- Contracts with **cloud computing applications** providers must address data retention, destruction, data ownership and data custodian rights.
- Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
- A general inventory of information (data) must be mapped and maintained on an ongoing basis.
- All SPPS assets must be formally classified with ownership assigned.
- Maintenance and repair of organizational assets must be performed and logged in a timely manner and managed by SPPS Technology Services Manager.
- SPPS assets exceeding a set value, as determined by management, are not permitted to be removed from SPPS 's physical premises without management approval.
- All SPPS physical assets exceeding a set value, as determined by management, must contain asset tags or a similar means of identifying the equipment as being owned by SPPS.
- If a SPPS asset is being taken to a High-Risk location (e.g. travel to China or Russia), as defined by the FBI and Office of Foreign Asset Control, it must be inspected and approved by Technology Services before being taken offsite and before reconnecting to the SPPS network.
- Confidential information must be transported either by an SPPS employee or a courier approved by Technology Services Management.
- Upon termination of employment, contract, or agreement, all SPPS assets must be returned to appropriate department leader and/or SPPS Technology Services Management.

Mobile Devices

- SPPS does not allow personally-owned mobile devices to connect to the SPPS corporate internal network.
- Mobile devices used to connect to the SPPS network are required to use the approved MDM solution.
- Mobile devices that access SPPS email must have a PIN or other authentication mechanism enabled.
- Confidential data should only be stored on devices that are encrypted in compliance with the SPPS Encryption Standard.
- All mobile devices should maintain up-to-date versions of all software and applications.

Media Destruction & Re-Use

- Media that may contain **confidential** or **internal information** must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
- Media reuse and destruction practices must be conducted in compliance with ISO/IEC 27002:2013(E) 8.3.2.
- All decommissioned media must be stored in a secure area prior to destruction.
- Media reuse and destruction practices must be tracked and documented.
- All information must be destroyed when no longer needed, included encrypted media.

Backup

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.
- The SPPS backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for SPPS must be formally approved to handle the highest classification level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest SPPS sensitivity level of information stored.
- A process must be implemented to verify the success of the SPPS electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss.
- Procedures between SPPS and the offsite backup storage vendor(s) must be reviewed at least annually.
- Backups containing **confidential information** must be encrypted.

Removable Media

- The use of **removable media** for storage of SPPS Information must be supported by a reasonable business case.
- All **removable media** use must be approved by SPPS Technology Services prior to use.
- **Personally-owned removable media** use is not permitted for storage of SPPS information.
- Users are not permitted to connect **removable media** from an unknown origin, without prior approval from SPPS Technology Services.
- Confidential and internal SPPS information should not be stored on **removable media** without the use of encryption.
- The loss or theft of a **removable media** device that may have contained SPPS information must be reported to the SPPS Technology Services.
- SPPS will maintain inventory logs of all **removable media** and conduct media inventories at least annually.
- The transfer of information to removable media may be monitored.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 6, 8, 11, 12, 16, 18
- NIST CSF: ID.AM, PR.IP, PR.DS, PR.PT, DE.CM
- SPPS Change Control Policy
- SPPS Information Classification and Handling Practices
- SPPS Encryption Practices

Waivers

Waivers from certain practice provisions may be sought following the SPPS Waiver Process.

Enforcement

Personnel found to have violated these practices may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated these practices may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	February 2018		FRSecure	Document Origination