Asset Management Policy

Purpose

The purpose of the (District/Organization) Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by (District/Organization).

Audience

The (District/Organization) Asset Management Policy applies to individuals who are responsible for the use, purchase, implementation, and/or maintenance of (District/Organization) Information Resources

Contents

|  |  |
| --- | --- |
| [Hardware, Software, Applications, and Data](#_Hardware,_Software,_Applications)  [Mobile Devices](#_Mobile_Devices)  [Media Destruction & Re-Use](#_Media_Destruction_&) | [Backup](#_Backup)  [Removable Media](#_Removable_Media) |

Policy

### Hardware, Software, Applications, and Data

* All hardware, software and applications must be approved and purchased by (District/Organization) IT.
* Installation of new hardware or software, or modifications made to existing hardware or software must follow approved (District/Organization) procedures and change control processes.
* All purchases must follow the defined (District/Organization) Purchasing Standard.
* Software used by (District/Organization) employees, contractors and/or other approved third-parties working on behalf of (District/Organization), must be properly licensed.
* Software installed on (District/Organization) computing equipment, outside of that noted in the (District/Organization) Standard Software List, must be approved by IT Management and installed by (District/Organization) IT 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 (District/Organization) 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 (District/Organization) 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 (District/Organization) IT Management.
* (District/Organization) assets exceeding a set value, as determined by management, are not permitted to be removed from (District/Organization)'s physical premises without management approval.
* All (District/Organization) 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 (District/Organization).
* If a (District/Organization) asset is being taken to a High-Risk location, as defined by the FBI and Office of Foreign Asset Control, it must be inspected and approved by IT before being taken offsite and before reconnecting to the (District/Organization) network.
* Confidential information must be transported either by an (District/Organization) employee or a courier approved by IT Management.
* Upon termination of employment, contract, or agreement, all (District/Organization) assets must be returned to (District/Organization) IT Management.

### Mobile Devices

* (District/Organization) does not allow personally-owned mobile devices to connect to the (District/Organization) corporate internal network.

OR

* The use of a personally-owned mobile device to connect to the (District/Organization) network is a privilege granted to employees only upon formal approval of IT Management.
* Mobile devices used to connect to the (District/Organization) network are required to use the approved MDM solution.
* Mobile devices that access (District/Organization) 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 (District/Organization) 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 (District/Organization)’s Information Reuse and Destruction Standards.
* 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 (District/Organization) backup and recovery process for each system must be documented and periodically reviewed.
* The vendor(s) providing offsite backup storage for (District/Organization) 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 (District/Organization) sensitivity level of information stored.
* A process must be implemented to verify the success of the (District/Organization) 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 (District/Organization) and the offsite backup storage vendor(s) must be reviewed at least annually.
* Backups containing **confidential information** must be encrypted.
* Signature cards held by the offsite backup storage vendor(s) for access to (District/Organization) backup media must be reviewed annually or when an authorized individual leaves (District/Organization).
* Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
  + - System name
    - Creation Date
    - Sensitivity Classification
    - (District/Organization) Contact Information

### Removable Media

* The use of **removable media** for storage of (District/Organization) Information must be supported by a reasonable business case.
* All **removable media** use must be approved by (District/Organization) IT prior to use.
* **Personally-owned** **removable media** use is not permitted for storage of (District/Organization) information.
* Users are not permitted to connect **removable media** from an unknown origin, without prior approval from (District/Organization) IT.
* Confidential and internal (District/Organization) 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 (District/Organization) information must be reported to the (District/Organization) IT.
* (District/Organization) will maintain inventory logs of all media and conduct media inventories at least annually.
* The transfer of information to removable media will 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
* (District/Organization) Change Control Policy
* (District/Organization) Information Classification and Handling Policy
* (District/Organization) Encryption Policy

Waivers

Waivers from certain policy provisions may be sought following the (District/Organization) Waiver Process.

Enforcement

Personnel found to have violated this policy 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 this policy 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 |  | SecurityStudio | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |