Asset Management Policy

Purpose

The purpose of the [Company Name] Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by [Company Name].

Audience

The [Company Name] Asset Management Policy applies to individuals who are responsible for the use, purchase, implementation, and/or maintenance of [Company Name] 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 [Company Name] IT.
* Installation of new hardware or software, or modifications made to existing hardware or software must follow approved [Company Name] procedures and change control processes.
* All purchases must follow the defined [Company Name] Purchasing Standard.
* Software used by [Company Name] employees, contractors and/or other approved third-parties working on behalf of [Company Name], must be properly licensed.
* Software installed on [Company Name] computing equipment, outside of that noted in the [Company Name] Standard Software List, must be approved by IT Management and installed by [Company Name] 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 [Company Name] 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 [Company Name] 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 [Company Name] IT Management.
* [Company Name] assets exceeding a set value, as determined by management, are not permitted to be removed from [Company Name]'s physical premises without management approval.
* All [Company Name] 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 [Company Name].
* If a [Company Name] 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 [Company Name] network.
* Confidential information must be transported either by an [Company Name] employee or a courier approved by IT Management.
* Upon termination of employment, contract, or agreement, all [Company Name] assets must be returned to [Company Name] IT Management.

### Mobile Devices

* [Company Name] does not allow personally-owned mobile devices to connect to the [Company Name] corporate internal network.

OR

* The use of a personally-owned mobile device to connect to the [Company Name] network is a privilege granted to employees only upon formal approval of IT Management.
* Mobile devices used to connect to the [Company Name] network are required to use the approved MDM solution.
* Mobile devices that access [Company Name] 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 [Company Name] 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 [Company Name]’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 [Company Name] backup and recovery process for each system must be documented and periodically reviewed.
* The vendor(s) providing offsite backup storage for [Company Name] 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 [Company Name] sensitivity level of information stored.
* A process must be implemented to verify the success of the [Company Name] 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 [Company Name] 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 [Company Name] backup media must be reviewed annually or when an authorized individual leaves [Company Name].
* 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
    - [Company Name] Contact Information

### Removable Media

* The use of **removable media** for storage of [Company Name] Information must be supported by a reasonable business case.
* All **removable media** use must be approved by [Company Name] IT prior to use.
* **Personally-owned** **removable media** use is not permitted for storage of [Company Name] information.
* Users are not permitted to connect **removable media** from an unknown origin, without prior approval from [Company Name] IT.
* Confidential and internal [Company Name] 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 [Company Name] information must be reported to the [Company Name] IT.
* [Company Name] 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
* [Company Name] Change Control Policy
* [Company Name] Information Classification and Handling Policy
* [Company Name] Encryption Policy

Waivers

Waivers from certain policy provisions may be sought following the [Company Name] 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 |  |  | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |