Information Security Document

Physical Asset Management Procedure

Version 1.0

Confidentiality and Usage statement

This Physical Asset management procedure document is the sole property of SRS solutions. It is provided for the internal usage and reference of employees, contractors, and authorized personnel associated with the organization.

The information contained in this document is considered confidential and proprietary to SRS solution. Unauthorized sharing, distribution, reproduction, or use of this document, in part or in its entirety, outside the scope of SRS solution's operations is strictly prohibited.

Any requests for sharing or distribution of this document beyond the organization's boundaries must be made in writing and approved by the management at SRS solution.

By accessing or using this document, you acknowledge your understanding of an agreement to comply with this confidentiality and usage statement.

SRS solution (Pvt) Ltd

1.Introduction and purpose

The physical infrastructure of SRS solutions addresses a range of equipment which addresses computers, servers, data centers and all other associated infrastructure. It is crucial to protect and maintain these infrastructures as they consist of sensitive data and hold a great deal in business continuity.

The purpose of this document is to explain the procedures related to the policies which are built up to protect and maintain the physical assets within the organization while addressing the responsible parties for the respective assets.

2.Scope

The included is relevant to all the employees (intern, contract based, permanent, outsource or other) who have access to the physical assets of SRS solutions. This document covers the complete life cycle of physical assets namely, usage, maintenance, deployment, and disposal.

3.Physical asset management policies

3.1 Asset inventory control policies

- Identification, classification, and documentation must be done for all the assets registered and owned by the company.

    - ✓ A centralized database for all the assets should be created.

    - ✓ Separate databases for separate asset categories should be created and the responsibility should be granted to the respective departments.
      E.g., User laptops and desktops – IT department, Security department
      Data center servers and other – Network department, Security department

    - ✓ Every asset should have a proper identification number.

- Asset ownership must be clearly defined and assigned to the relevant individual or department.

    - ✓ Databases should consist of the ownership of the asset (Individual or the department) with his name, address, designation, and other important details.

- ✓ Relevant individuals or the department personnel should sign a written document before taking ownership of the assets.
- ✓ It is compulsory for the security department to keep the record of ownership of all data critical assets.
- ✓ Once the asset is returned the ownership should be immediately terminated and updated with the relevant department initially responsible for the respective asset when it is not assigned to anyone.
  E.g., Once a user returns a laptop IT department should take the full responsibility of the laptop until it is given back to another user.

3.2 Asset monitoring and tracking policies

- Asset location and must be recorded in the inventories during registration.

  - ✓ Asset location must be recorded in the databases once it is registered.
  - ✓ The current location of the asset should be updated once changed.

- Assets like computers, laptops, tablets and likewise must be added to the cloud active directory domain.

  - ✓ The IT department is responsible for handing over the laptops and tablets to the respective user only after adding to the company domain so that the latest user can be monitored using azure active directory if any user inside the company domain uses the asset.

- Serial numbers of devices like servers, laptops, computers, tablets and likewise must be recorded at the registration.

  - ✓ Serial numbers should be recorded at the asset registration for the applicable assets to track if a device loss occurred. Department which has the initial official right over the item is responsible for recording the serial number in the database.

- Physical asset audits must be carried out on a regular basis to confirm the asset inventory's accuracy and completeness. Any discrepancies must be resolved quickly.

  - ✓ Begin by examining and approving the policy for performing physical asset audits. Ensure that all essential stakeholders, including management and audit teams, are on board.
  - ✓ Create a regular audit schedule that specifies when and how frequently physical asset audits will be performed. When deciding the frequency, consider the size and complexity of your asset inventory.

- ✓ Form an audit team that will oversee conducting the audits. Define team members' roles and responsibilities, including the audit lead, data recorder, and verifier.
- ✓ Create an audit checklist and thorough audit procedures outlining what should be verified during the audit. Asset tags, serial numbers, condition, location, and other pertinent information may be included.
- ✓ Notify the appropriate departments or people about the planned audit in advance. During the audit, they should be prepared to offer the appropriate access and information.
- ✓ Physically inspect assets during the audit to confirm their presence, location, condition, and any identifying information (such as asset tags or serial numbers).
- ✓ Record asset data, including any anomalies or abnormalities detected throughout the audit, using the audit checklist.
- ✓ Make certain that all audit findings and data obtained are appropriately documented and recorded. This information should be entered into the asset register or database.
- ✓ Create a clear procedure for addressing disagreements. Outline the actions for investigating and resolving the issue if an asset is discovered to be missing or damaged. Notifying the proper department, conducting follow-up audits, or taking corrective steps may be included.
- ✓ Produce an audit report that summarizes the findings and indicates any inconsistencies. The audit lead and management should examine and approve this report.
- ✓ Define the corrective measures that must be implemented in response to the audit results. Ordering replacements, updating asset data, and modifying asset tracking methods are all examples of this.
- ✓ Inform the audit team and other relevant stakeholders on the audit procedures and the need for precise asset tracking. Ascertain that they are aware of their roles in the auditing process.
- ✓ Review the audit process and processes on a regular basis to incorporate input and make necessary modifications.
- ✓ Implement security measures to prevent unauthorized access or tampering with audit data and reports. Only authorized personnel should have access.
- ✓ Install a records management system to securely archive and store all audit-related documents and reports.
- ✓ Create protocols for dealing with asset-related emergencies uncovered during the audit, such as theft, loss, or damage to assets.

3.3Access Control Policies

- Physical access controls should be allowed only for the authorized personnel to the areas consisting critical physical assets (Eg: Server rooms, data centers)

- ✓ Should take measures to make sure only authorized personnel enter the areas consisting critical assets.
- ✓ Only the authorized members of the Security Department and Network Department are allowed inside the datacenter.
- ✓ Even the authorized member should only enter the server rooms or data center premises with a valid reason (E.g., Hardware upgrade, server installation)
- ✓ The fingerprint machine in front of the data center or the server room should be programmed so that the door opens only when the authorized member puts their fingerprint on.
- ✓ The same applies to all other locations consisting critical assets.
- ✓ Ensure that surveillance cameras with a lens capturing the essential focal area clearly be fixed at the areas consisting critical physical assets.
- ✓ Use recommended grade fences to prevent any unauthorized person's illegal entry.

- Access to sensitive physical assets should undergo proper authentication and authorization.
-
    - ✓ Access to the critical assets should be done with proper authentication and authorization.
    - ✓ The Security department is responsible for implementing the role-based access controls within the company.
    - ✓ The responsible personnel should
        - Define the roles properly (E.g., CEO, manager, salesperson, IT head)
        - Assign permission.
        - Assign User roles.
        - Apply access control based on roles defined.
        - Review role-based access control periodically
        - Establish role hierarchies (If applicable)
        - Log and audit

- Employee access to the physical assets must be removed once resigned, fired or under other considerable circumstances.

    - ✓ The security department is responsible for ensuring that the access of the user is revoked based on the above circumstances.
    - ✓ This should be done immediately under the mentioned circumstances.
    - ✓ The department of the user is responsible for providing a clear report to the security department mentioning the details of physical assets the user consumed which requires revocation.

3.4 Asset maintenance and security policies

- Physical assets must be regularly maintained and must ensure the integrity and security of them.

    - ✓ All the physical assets must be maintained accordingly.
    - ✓ For the devices which are handed over to the users for official usage, proper guidelines for using them should be given by the responsible department.

      E.g. When laptops are given to the user by the IT department proper guidelines should be given to the user on how to maintain the device. For example, the department can provide a written set of guidelines mentioning directions like restarting the laptop daily likewise.

    - ✓ Documented guidelines should be provided when it comes in maintaining the cleanliness of sensitive devices like data center servers, switches, routers and so on. Staff should be trained to clean them without damaging the devices.
    - ✓ Devices should be properly disposed and replaced at the correct time which will be elaborately explained in further sections.

- Implement surveillance systems, alarm systems and other environmental controls to protect physical assets from threats like theft, damage, and unauthorized access.

    - ✓ Surveillance cameras should be placed accordingly around the places with critical physical assets.
    - ✓ Ensure that the cameras are working properly and should be immediately repaired or replaced if damaged or not in working state.
    - ✓ Analyze the environment and place gates and fences suiting to proper standard to prevent from unauthorized entry. Recommended to take suitable advice from experts related this.
    - ✓ Implement proper alarm systems to protect the critical assets.

      E.g.:
      - Fire alarm systems should be installed, and their functionalities should be tested accordingly.
      - In case of security attack to any data critical physical infrastructure (Server, Router), the alarm system should be implemented to alert the security team.
      - Proper alarm systems should be implemented if there is an unauthorized entry.

    - ✓ Place fire extinguishers accordingly at each floor of the building.

- Security updates and software patching should be done to applicable assets.

- ✓ Security team is responsible for pushing security updates to the users through corporate domain.
- ✓ Users should be made aware about and pre notified before these updates.
- ✓ Server security updates should be done accordingly with properly scheduled downtimes (if required).

- For remote employees using company physical assets (Laptops, Tablets etc.), necessary actions should be taken to protect the assets from security threats. (E.g., Access to VPN for sensitive tasks)

    - ✓ Provide remote employees with access to a Virtual Private Network (VPN) for secure and encrypted connections to the company network, particularly for sensitive tasks.
    - ✓ Train employees on how to connect to the VPN and the importance of using it for sensitive data transmission.
    - ✓ Install and regularly update endpoint security software (antivirus, antimalware) on company devices to detect and prevent security threats.
    - ✓ Enable firewall and intrusion detection systems for an additional layer of protection.
    - ✓ Ensure that operating systems and software applications on company devices are regularly updated to patch security vulnerabilities.
    - ✓ Establish a procedure for remote employees to apply updates promptly.
    - ✓ Implement a Mobile Device Management system to remotely manage and secure mobile devices (smartphones, tablets) issued to employees.

3.5Asset Disposal and Decommissioning policies

- Assets should be disposed after the recommended usage time has passed.

    - ✓ The recommended usage period for any electronic asset is five years. It is compulsory to remove the assets after this time.
    - ✓ Non electronic assets may have different expire period. Therefore, they should be disposed after the recommended period.
- The disposal list must be accurately listed and signed by the responsible personnel before disposal of the assets.
    - ✓ The relevant department should take the responsibility on making the disposal list. E.g.: IT department should take the responsibility

      - Making the list of the items past five years.
      -Informing the relevant users to return those items back to IT department.
      -Replacing them with new laptops.

-Backing up critical user data with user's negotiation and feeding them into their new device
-Getting the approval from the department head and the financial department and handing it over to the responsible HR personnel for disposal.

- Required data should be backed up and all the data should be wiped or destroyed before disposal.

  - ✓ All the data should be completely erased before disposal. Critical data should be backed up accordingly.

    Identify Data to Backup:

    -Determine the electronic assets (e.g., computers, smartphones, servers) from which data needs to be backed up before disposal.

    -Identify the types of data to be preserved (e.g., documents, emails, settings, applications).

    Data Backup:

    -Choose a secure and reliable backup method, such as cloud storage, external hard drives, or network-attached storage (NAS).
    -Ensure the backup solution is encrypted and password-protected to maintain data security during transfer and storage.

    Verify Backup Integrity:

    - After backing up data, verify the integrity of the backup to ensure no data loss occurred during the process.
    - Confirm that all essential files and settings have been successfully copied.

    Data Wiping/Destroying:

    -Determine the method to be used for data wiping or destruction, depending on the type of device and your organization's security policies.
    -Options include data wiping software, physical destruction (e.g., shredding hard drives), or secure erasure services.

    Data Wiping Software:

    - If data wiping software is used, ensure it complies with recognized data sanitization standards (e.g., NIST, DoD 5220.22-M).

-Run the wiping software on the electronic assets, erasing all stored data.

Secure Storage:

-If electronic assets are not immediately sent for disposal, store them securely in a designated area to prevent unauthorized access to the data.

Documentation:

-Maintain detailed records of the data backup, wiping, and destruction process, including the devices involved and the method used.
Keep copies of certificates of data sanitization.

Employee Training:

-Train employees on the importance of data security and the procedures for secure data backup and disposal.

Periodic Review:
-Regularly review and update the data backup and disposal procedures to ensure they remain effective and compliant with relevant regulations.

- Disposal of electrical and electronic assets should follow proper environmental standards when disposing.

  - ✓ Examine national, state, and local e-waste disposal rules.
  - ✓ Comply with the Waste Electrical and Electronic Equipment (WEEE) directive and any applicable local regulations.
  - ✓ Determine which assets are still functional and can be repurposed.
  - ✓ Consider donating or selling these assets to individuals or organizations in need.
  - ✓ Speak with accredited e-waste recycling firms or recycling sites that follow environmental regulations.
  - ✓ Ensure that the facility of choice has the relevant certifications for responsible e-waste management.
  - ✓ Make arrangements for the safe transfer of e-waste to a recycling center.
  - ✓ Protect products from physical harm and environmental dangers during transit.
  - ✓ Separate and secure e-waste from other waste streams to avoid contamination.
  - ✓ E-waste recycling facilities will typically disassemble and recycle e-waste components.
  - ✓ Precious metals and materials are separated for recycling, and hazardous components are appropriately treated.

- ✓ Keep meticulous records of the disposal procedure, including the goods discarded, their condition, and the recycling facility used.
- ✓ Document environmental compliance and data sanitization methods.
- ✓ Consider tracking and reporting on your e-waste disposal operations' environmental impact, such as carbon footprint reduction or resource conservation.
- ✓ Aware staff of the significance of proper e-waste disposal and encourage them to report any e-waste disposal requirements that arise within the organization.
- ✓ Review and update your e-waste disposal methods on a regular basis to maintain continued compliance with new environmental standards.

4.Physical asset management awareness policies

- Users of physical devices must be given a proper awareness before handing it over.

  -Create a comprehensive set of user guidelines and policies that outline the responsible use of physical devices.
  -Include information on device security, data protection, and acceptable use.
  -Require users to sign an agreement confirming that they have received the physical device and have been made aware of the guidelines and policies.
  -Ensure that users understand the terms and conditions outlined in the agreement.
  - Educate users on proper device handling, care, and maintenance to extend the device's lifespan.
  -Encourage the use of protective cases, screen protectors, and proper charging practices.
  - Instruct users on secure Wi-Fi connections and the use of Virtual Private Networks (VPNs) if necessary for remote work.
  -Advise against connecting to unsecured public Wi-Fi networks
  - Teach users the importance of strong, unique passwords for device access.
  - Encourage the use of biometric authentication methods when available.

- Security awareness sessions must be held to make the employees aware of security threats which can affect their physical assets like office laptops, tablets etc.

  -Schedule an orientation session for users to provide them with the physical devices.
  -During this session, cover the following topics:

  i. Device functionality and features.
  ii. Security measures and guidelines for safe usage.
  iii. Data protection practices, including data backup and encryption.
  iv. Compliance with company policies and relevant regulations.
  v. Reporting procedures for loss, theft, or security incidents.
  vi. User responsibilities and expectations.

5.Roles and responsibilities

- The SRS security team is responsible for implementing and enforcing the policies and procedures.
- Security auditor and the management is responsible for negotiating and approving the policies and procedures.
- All the employees are responsible for complying with the policy and reporting of any suspected violations.

6.Procedure Review

This procedure document should be reviewed annually and should be updated according to the prevailing circumstances at that time.

7.Procedure Approval

This procedure has been reviewed and approved by the SRS solution's management and security auditor.

Date of Approval: 11/2/2023
Approved By: Security Auditor and SRS management.
SRS Solution,
Malabe, Sri Lanka
0378976554