Information Security Document

Physical Asset Management Policy

Version 1.0

Confidentiality and Usage statement

This Physical Asset management policy 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 establish policies 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.
- Asset ownership must be clearly defined and assigned to the relevant individual or department.

3.2 Asset monitoring and tracking policies

- Asset location and must be recorded in the inventories during registration.
- Assets like computers, laptops, tablets and likewise must be added to the cloud active directory domain.
- Serial numbers of devices like servers, laptops, computers, tablets and likewise must be recorded at the registration.
- 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.

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)
- Access to sensitive physical assets should undergo proper authentication and authorization.
- Employee access to the physical assets must be removed once resigned, fired or under other considerable circumstances.

3.4 Asset maintenance and security policies

- Physical assets must be regularly maintained and must ensure the integrity and security of them.
- Implement surveillance systems, alarm systems and other environmental controls to protect physical assets from threats like theft, damage, and unauthorized access.
- Security updates and software patching should be done to applicable assets.
- For remote employees using company physical assets (Laptops, Tablets etc), necessary actions should be taken to protect the assets from security threats. (Eg: Access to VPN for sensitive tasks)

3.5Asset Disposal and Decommissioning policies

- Assets should be disposed after the recommended usage time has passed.
- The disposal list must be accurately listed and signed by the responsible personnel before disposal of the assets.
- Required data should be backed up and all the data should be wiped or destroyed before disposal.
- Disposal of electrical and electronic assets should follow proper environmental standards when disposing.

4.Physical asset management awareness policies

- Users of physical devices must be given a proper awareness before handing it over.
- Security awareness sessions must be held to make the employees aware of security threats which can affect the physical assets like office laptops, tablets etc.

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.
- Further responsibilities related to each policy will be elaborately discussed in the procedure document.

6.Policy Review

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

7.Policy Approval

This policy 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