Sarva Seva Samity Sanstha- 4S India

Data Security Policies

This document provides data securitypolicies that cover key areas of concern for 4s India .

The three policies cover:

1. Datasecuritypolicy:Employee requirements
2. Datasecuritypolicy:DataLeakagePrevention–Data inMotion
3. Datasecuritypolicy:WorkstationFullDisk Encryption

Comments to assist in the use of these policies have been highlighted

Data security policy: Employee requirements

Using this policy

This example policy outlines behaviors expected of employees when dealing with data and provides a classification of thetypesof data with which theyshould be concerned.This should link to your AUP (acceptableuse policy), security trainingandinformation security policy to provide users with guidance on the required behaviors.

1.0 Purpose

4S must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impactingourcustomers.The protectionofdataisacriticalbusinessrequirement,yetflexibilitytoaccessdataand work effectively is also critical.

It isnot anticipatedthatthistechnologycontrolcaneffectivelydealwiththe malicious theft scenario,or thatit willreliablydetect alldata.It's primaryobjectiveis userawarenessandto avoid accidentallossscenarios.This policy outlines therequirementsfor data leakage prevention, a focus for the policy and a rationale.

2.0 Scope

1. Any employee, contractor or individual with access to 4S systems or data.
2. Definition of data to be protected
    - PII
    - Financial
    - Restricted/Sensitive
    - Confidential
    - IP

3.0 Policy – Employee requirements

1. Need to complete 4S's security awareness training and agree to uphold the acceptable use of policy.
2. If you identify an unknown, un-escorted or otherwise unauthorized individual in 4S you need to immediately notify
   Respective Reporting Officer (RO).
3. Visitors to 4S must be escorted by an authorized employee at all times. If you are responsible for escorting visitors you must restrict those appropriate areas.
4. You are required not to reference the subject or content of sensitive or confidential data publically, or via systems or communication channels not controlled by 4S.
5. Please keep a clean desk. To maintain information security you need to ensure that all printed data is not left unattended at your workstation.
6. You need to use a secure password on all 4S systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
7. Terminated employees will be required to return all records, in any format, containing personal information.
8. You must immediately notify in the event that a device containing data is lost (e.g. mobiles, laptops etc).
9. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform RO, so that they can take appropriate action.
10. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from RO if you are unsure as to your responsibilities.
11. Please ensure that assets holding data are not left unduly exposed, for example visible in the back seat of your car.
12. Data that must be moved within 4S is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). 4S will provide you with systems or devices that fit this purpose. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with RO.
13. Any information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations.

Data security policy: Data Leakage Prevention (DLP) – Data in Motion

Using this policy

This example policy is intended to act as a guideline for organizations looking to implement or update their DLP controls. Adapt this policy, particularly in line with requirements for usability or in accordance with the regulations or data you need to protect. This policy provides a framework for classes of data that may wish to be monitored. You should expand them to cover the sensitive assets in your business and subject to the types of you hold.

Background to this policy

Dataleakagepreventionisdesignedtomakeusersawareof datatheyare transferring which maybesensitive or restrictedin nature.

1.0 Purpose

4S must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impactingour customers.The protection ofin data isa criticalbusiness requirement, yetflexibility to accessdataandwork effectively is also critical.

2.0 Scope

1. Any 4S device which handles customer data, sensitive data, personally identifiable information or company data. Any device which is regularly used for e-mail, web or other work related tasks and is not specifically exemptforlegitimate business or technology reasons.
2. The 4S information security policy will define requirements for handling of information and user behaviour requirements.Thispolicyistoaugmenttheinformationsecuritypolicywithtechnologycontrols.
3. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted being authorized by security management.

3.0 Policy

1. 4S's DLP technology will scan for data in motion.
2. The DLP technology will identify large data. A large number of records is defined as <complete as appropriate.
   a. Credit card details, bank account numbers and other financial identifiers
   b. E-mail addresses, names, addresses and other combinations of personally identifiable information
   c. Documentsthathavebeenexplicitlymarkedwiththe'4SConfidential'string.
3. DLP will identify specific content, i.e.:
   a. Sales data – particularly forecasts, renewals lists and other customer listings
   b. Exports of personally identifiable information outside controlled systems.
4. DLP will be configured to alert the user in the event of a suspected transmission of sensitive data, and the user will be presented with a choice to authorize or reject the transfer. This allows the user to make a sensible decision to protect the data, without interrupting business functions. Changes to the DLP product configuration will be handled through the
   4S IT change process and with security management approval, to identify requirements to adjust the information security policy or employee communications.

5. DLP will log incidents centrally for review. The IT team will conduct first level triage on events, identifying data that may be sensitive and situations where its transfer was authorized and there is a concern of inappropriate use. These events will be escalated to HR to be handled through the normal process and to protect the individual..
6. Where there is an active concern of data breach, the IT incident management process is to be used with specific notification provided to RO.
7. Access to DLP events will be restricted to a named group of individuals to protect the privacy of employees. A DLP event does not constitute evidence that an employee has intentionally, or accidentally lost data but provides sufficient basis for investigation to ensure data has been appropriately protected.

Data security policy: Workstation Full Disk Encryption

Using this Policy

This example policy is intended to act as a guideline for organizations looking to implement or update their full disk encryption control policy. Adapt this policy, particularly in line with requirements for usability or in accordance with the regulations or data you need to protect.

Background to this policy

Full disk encryption is now a key privacy enhancing technology which is mandated my many regulatory guidelines.

1.0 Purpose

4S must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. As defined by numerous compliance standards and industry best practice, full disk encryption is required to protect against exposure in the event of loss of an asset. This policy defines requirements for full disk encryption protection as a control and associated processes.

2.0 Scope

1. All 4S work stations – desktops and laptops.
2. All 4S virtual machines.

3.0 Policy

1. All devices will have full disk encryption enabled.
2. The Acceptable Use Policy (AUP) and security awareness training must require users to notify of any device which is lost or stolen.
3. Encryption policy must be managed and compliance validated. Machines need to report to the central management infrastructure to enable audit records to demonstrate compliance as required.
4. Where management is not possible and a standalone encryption is configured, the device user must provide a copy of the active encryption key to IT.
5. 4S has the right to access any encrypted device for the purposes of investigation, maintenance or the absence

of an employee with primary file system access.

6. The encryption technology must be configured in accordance with industry best practice to be hardened against attacks.
7. All security related events will be logged and audited by <complete as appropriate> to identify inappropriate access to systems or other malicious use.
8. The 4S helpdesk will be permitted to issue an out-of-band challenge/response to allow access to a system in the event of failure, lost credentials or other business blocking requirements. This challenge/response will be provided only in the event that the identity of the user can be established using challenge and response attributes documented in the password policy.
9. Configuration changes are to be conducted through the IT company, having contract, change control process, identifying risks and noteworthy implementation changes to security management.

(revised as on 3oth sep, 23)

==========end==========