SECURIYTY POLICY

RIHAM AHAMED ABDUL RAHEEM
HND COMPUTING IDM

Contents

Fundamentals

The safety and protection of assets, facilities, employees and customers is fundamental to the effective and efficient working of the practice. This Policy provides a framework and a very strict guideline which allows us to manage the aforementioned resources in the most secure manner while maintaining efficiency.

“The security of UniCare is the responsibility of everyone, all employees subjected under the policy and any involved parties who have read the policy must enforce the policy as is in the mentioned magnitude”.

Scope

To meet legal and professional requirements the practice must use cost effective security measures to safeguard all of its resources.This Security Policy will ensure a consistent approach to the implementation of appropriate security controls against common and expected threats.

Policy Control

Only the highest ranking security officer in UniCare except the author is allowed to make changes to the policy. If ever there comes a need to do so, depending on the magnitude of the change to the policy if the management panel of UniCare has granted authority through majority vote, the author does not have be contacted compulsorily, however if not, failure in contacting the author to request permission to change the policy will be treated as treason and charged with a law suit.

Overview

The policy will cover the following topics in great detail:

- General practices
- Orientation and training
- Physical Security
- System access control
- Malicious software & preventive methods
- ISO 33001: Risk Management
- Data protection act

Risk & Vulnerability management

All employees must be trained in understanding the significance of a risk, threat and vulnerability. UniCare must see that they adhere to Sri Lanka's Data Protection Act(2018) and Risk Management ISO:31000 documents while engaging in transactions.

- All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices such as CVSS base score.
- As part of the company requirements, UniCare will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Quarterly internal vulnerability scans must be performed by UniCare by internal staff or a 3rd party vendors and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities are resolved.
- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by the company's internal staff. The scan process should include re-scans until passing results are obtained.

General information security

UniCare handles sensitive customer information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect customer privacy, to ensure compliance with various regulations and to guard the future of the organization.

UniCare commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process customer information so that we can meet these promises.

- Handle company and customer information in a manner that fits their sensitivity.
- Limit personal use of UniCare information and telecommunication systems and ensure it doesn’t interfere with your job performance.
- UniCare reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.
- Do not use e-mail, internet and any other company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
- Do not disclose personnel information unless authorized.
- Keep passwords and accounts secure.
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.
- Do not install unauthorized software or hardware, including modems and wireless access unless you have explicit management approval.
- Always leave desks clear of files that may contain sensitive data and lock computer screens when unattended.
- ALL security incidents must be reported, without delay, to the individual(s) responsible for that department locally – it is well advised to identify who the individual(s) are.

The management’s intentions for publishing a policy are not to impose restrictions that are contrary to UniCare established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.

- Employees should ensure that technologies should be used and setup in acceptable network locations
- Keep passwords secure and do not share accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of UniCare, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, or Trojan code.

Physical Security

Resources associated within the practice, including office machinery, IT equipment and the company building(s) shall be protected from unauthorized access, misuse, damage or theft. Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies. Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations

  A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device

- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices.
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behavior and indications of tampering of the devices to the appropriate personnel.
- An “external party” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive customer information must be handled and distributed in a secure manner by trusted individuals.
- External parties must always be escorted by a trusted employee when in areas that hold sensitive customer information.
- Procedures must be in place to help all personnel easily distinguish between employees and external parties, especially in areas where customer data is accessible.
- Network Jacks located in public and areas accessible to external parties must be disabled and enabled when network access is explicitly authorized.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive customer data must have a password protected screensaver enabled to prevent unauthorized use.

System Access Control

Access Control systems are in place to protect the interests of all users of UniCare computer systems by providing a safe, secure and readily accessible environment in which to work.

- UniCare will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification
- Access to The Company IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any The Company IT resources and services will be provided without prior authentication and authorization of a user's UniCare Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorized persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.

- Users are expected to become familiar with and abide by UniCare policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.

Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary. A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

Password eligibility and maintenance

All users, including contractors and vendors with access to UniCare systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Herein, all passwords stored in a database must be salted, hashed and encrypted before storing, in the case of a usage of key-based encryption, the key must be stored securely, and all decryption utilities must be thoroughly checked and tested for vulnerabilities.

- A system configuration standard must be developed along industry acceptable hardening standards which must be one of SANS, NIST or ISO.
- System configurations should be updated as new issues are identified (as defined in PCI DSS requirement 6.1)
- System configurations must include common security parameter settings
- The systems configuration standard should be applied to any news systems configured.
- All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into UniCare network and all unnecessary services and user/system accounts have to be disabled.

- All unnecessary default accounts must be removed or disabled before installing a system on the network.
- Security parameter settings must me set appropriately on System components
- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.
- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
- Any insecure protocols, daemons, services in use must be documented and justified.
- All users with access to card holder data must have a unique ID.
- All users must use a password to access the company network or any other electronic resources
- All user ID's for terminated users must be deactivated or removed immediately.
- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.
- All system and user level passwords must be changed on at least a quarterly basis.
- A minimum password history of four must be implemented.
- A unique password must be setup for new users and the users prompted to change the password on first login.
- Group, shared or generic user account or password or other authentication methods must not be used to administer any system components.
- Where SNMP (Simple Network Management Protocol) is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.
- All non-console administrative access will use appropriate technologies like SSH and VPN or strong encryption(AES256, Blowfish) is invoked before the administrator password is requested
- System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands

- Administrator access to web based management interfaces is encrypted using strong cryptography.
- The responsibility of selecting a password that is hard to guess generally falls to users.

  A strong password must:

  a) Be as long as possible (never shorter than 6 characters).
  b) Include mixed-case letters, if possible.
  c) Include digits and punctuation marks, if possible.
  d) Not be based on any personal information.
  e) Not be based on any dictionary word, in any language
- If an operating system without security features is used (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.
- To protect against network analysis attacks, both the workstation and server should be cryptographically secured ex: encrypted Netware login and Kerberos.

Security awareness & training procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form.
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the company.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- All employee details of who have read the policy must be recorded by a high ranking security officer in UniCare.
- Company security policies must be reviewed annually and updated as needed as long as the aforementioned rule of granting permission has been fulfilled.

If an employee is found going against the policy, or has been reported as such, he/she shall be interrogated as to the reasoning behind his/her actions.

Then upon completion of the interrogation(when necessary proof has been gathered or if the subject has confessed), the management panel will decide the involved party’s punishment and through majority vote come to a decisive conclusion. If the management fails to do so, by default 2% for minor situations to 25% to extreme situations of the involved party’s salary in the month the action took place shall be deducted.

If during the interrogation it is revealed that the action was not intentional or that the employee did not know the policy contained such standards, then the management should take action to train the employee. However if it is later revealed that the employee has falsified upon checking the records, then the employee must be punished additionally for falsifying which is again under the hands of the management panel.

Auditing & Log reviews

This procedure covers all logs generated for systems within the cardholder data environment, based on the flow of cardholder data over UniCare network, including the following components:

- Operating System Logs.
- Database Audit Logs.
- Firewalls & Network Switch Logs.
- IDS Logs.
- Antivirus Logs.
- CCTV Video recordings.
- File integrity monitoring system logs.

- Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline.
- Review of logs is to be carried out by means of UniCare's network monitoring system, which is controlled from UniCare console. The console is installed on the server (the Company to define hostname / IP address), located within UniCare data centre environment.
- UniCare should hold a meeting to decide who reviews what logs.
- The network monitoring system software used must be configured to alert UniCare administrators to any conditions deemed to be potentially suspicious, for further investigation. Alerts are configured to: • A dashboard browser-based interface, monitored by the company administrators.
- Email/SMS alerts to UniCare administrators mailbox with a summary of the incident. The company administrators also receive details of email alerts for informational purposes.
- The following Operating System Events are configured for logging, and are monitored by the console

  a) Any additions, modifications or deletions of user accounts.

  b) Any failed or unauthorized attempt at user logon.

  c) Any modification to system files.

d) Any access to the server, or application running on the server, including files that hold cardholder data.

e) Actions taken by any individual with root or administrative privileges.

f) Any user access to audit trails.

g) Any creation / deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

- The following Database System Events are configured for logging, and are monitored by the network monitoring system:

a) Any failed user access attempts to log in to the database.

b) Any login that has been added or removed as a database user to a database.

c) Any login that has been added or removed from a role.

d) Any database role that has been added or removed from a database.

e) Any password that has been changed for an application role.

f) Any database that has been created, altered, or dropped.

g) Any database object, such as a schema, that has been connected to.

h) Actions taken by any individual with DBA privileges.

- The following Firewall Events are configured for logging, and are monitored by the network monitoring system:

a) Access Control List violations.

b) Invalid user authentication attempts.

c) Logon and actions taken by any individual using privileged accounts.

d) Configuration changes made to the firewall.

- The following Switch Events are to be configured for logging and monitored by the network monitoring system:

a) Invalid user authentication attempts.

b) Logon and actions taken by any individual using privileged accounts.

c) Configuration changes made to the switch.

- The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system:
  a) Any known denial of service attack(s).
  b) Any traffic patterns that indicated pre-attack reconnaissance occurred.
  c) Any attempts to exploit security-related configuration errors.
  d) Any authentication failure(s) that might indicate an attack.
  e) Any traffic to or from a back-door program.
  f) Any traffic typical of known stealth attacks.
- The following File Integrity Events are to be configured for logging and monitored by:
  a) Any modification to system files.
  b) Actions taken by any individual with Administrative privileges.
  c) Any user access to audit trails.
  d) Any Creation / Deletion of system-level objects installed by Windows.
- For any suspicious event confirmed, the following must be recorded on a logs review form, and UniCare administrators must be informed:
  a) User Identification.
  b) Event Type.
  c) Date & Time.
  d) Success or Failure indication.
  e) Event Origination (specially IP address).
  f) Reference to the data, system component or resource affected.

Anti-virus software

All machines must be configured to run the latest anti-virus software as approved by UniCare. The preferred applications to use are the Malware Bytes robust antimalware alongside Kaspersky antivirus, the antivirus should have periodic scanning enabled for all the systems.

- The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits).
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- All removal of malicious entities must be logged and handled as mentioned in the policy.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements for at least 3 months online and 1 year offline.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans
- End users must not be able to modify and any settings or alter the antivirus software
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

Disposal of data

All data must be securely disposed of when no longer required by Active Insurance Services, regardless of the media or application type on which it is stored.

- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of customer data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic customer data has been appropriately disposed of in a timely manner.
- UniCare will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- UniCare will have documented procedures for the destruction of electronic media.
- All customer information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” -access to these containers must be restricted.