Password Policy

Overview

Passwords are an important aspect of computer security and are considered as a frontline of protection for user accounts. A weak password may result in compromising entire SITS Group's corporate network. As such, all the SITS Group employees (including contractors and vendors with access to the SITS Group systems) are responsible for taking appropriate steps as outlined below to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of such passwords, and the frequency for changing passwords.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any of the SITSGroup facility and has access to SITS Group network.

Policy

General

- All system-level passwords (e.g., root, enable, Domain admin, application administration accounts, etc.) must be changed at least on monthly basis or as mandated by Exchanges or Regulators from time to time.
- All production system-level passwords must be part of the I.T. department administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Contain both upper- and lower-case characters (e.g., a-z, A-Z)
- Have digits, punctuation or special characters as well as letters e.g., 0-9,!@#$ %^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.

User Management and Access Control Policy

Purpose

The purpose of this policy is to establish a standard for maintenance of concrete logs for various applications/systems and maintaining record of user activity thereby ensuring users are authenticated and identified so that they can be held accountable for their actions

Scope

The scope of this policy includes all personnel who have or are responsible for use, manage, design or implement programs and has access to the SITS Group Technology network.

Policy

The following functions must be recorded:

- log-in attempts,
- password changes, and
- file creations, changes and/or deletions.
- The audit trail event record should specify:
- type of event,
- when the event occurred,
- user ID associated with the event, and
- program or command used to initiate the event.

Audit trails must be reviewed by the System Administrator. The IT Team must review the audit trail monthly.

Anomalies must be immediately reported to appropriate supervisory/IT Manager and/or system provides for follow-up action.

All audit files shall be stored on the secured network drive and kept for five years.

Firewall Rules and Implementation Policy

The purpose of this policy is to establish an understanding of the role that the firewall plays in the overall security of SITS's network and day to day smooth functioning of business applications and messaging systems.

Guidelines:
Changes to the firewall need to be done only post market hours and during non- critical business hours.

The configuration file of the firewall is backed up before adding a new policy or making any changes to the existing rules.
The proposed new rule addition is discussed internally within the IT Team and with the application vendor if required.
After addition of rules to firewall, the important rules/policies like POP3, SMTP and VPN connectivity are cross checked.

1. Purpose:

The purpose of this policy is to engage the IT Team in good practices with respect to Network Infrastructure as it is an important component of ensuring the potential threats to the overall Network Architecture and its security are managed effectively.

2. Scope:

The scope of this policy applies to the IT Team and its Department Head.

3. Guidelines:

The following security principles should be followed:

- Network devices should be configured securely and accessed in a secured manner
- Secure protocols should be used for network communications
- Internal and external facing networks should be appropriately segregated through the use of
- demilitarized zones (DMZs) and control devices such as securely configured firewalls or router Access
- Control Lists
- Remote access to internal networks should be managed securely
- Internal networks should be configured to prevent or detect attempted unauthorized connections and the flow of suspicious traffic

3.1 Internal LAN requirements:

The architecture of internal networks should enforce the separation of different types of networked systems (such as workstations and servers) into distinct VLANs or DMZ, and routing should be enabled to allow for communication between DMZs and the creation and management of isolated security segments.

3.2 Network Connection Control

An explicit rule is to be added to ensure that all workstations and servers cannot connect directly to the Internet; connections to the Internet should take place through the firewall.
A rule or number of rules should be added to ensure that all workstations can connect to the appropriate servers required for proper functionality, such as file, print, application and e-mail servers. If further access control to resources is required (for example, access to file shares needs to be restricted on a per-user basis) this should be implemented through the use of Active Directory setup.

3.3 Administrative Services

It is recommended that the availability of administrative services on Network Systems and devices is restricted to authorized internal IP addresses.

3.4 External Connection requirements

It is imperative that in the event of any external party or Vendor requires in-bound access to SITS's internal networks via Internet, access is not granted to third parties unless the IT Manager determines that there is a legitimate need for such access. If there is a legitimate need for access, the access should only be granted for the time period required for the 3rd party to accomplish their approved tasks.

3.5 Network Devices Configuration

3.5.1 Firewall

- Implement an explicit deny rule if no other rules are matched
- All filtering rules should be implemented to only allow traffic that is in line with business operations.
- These rules should be configured explicitly with source, destination and network port number for each rule
- Ensure that generic logins are not used to authenticate to the firewall's administrative console
- Do not include any "allow all" rules

- In addition, firewall configuration and permissible service rules should not be changed unless the permission of the IT Head
- Content filters should use a combination of “black lists” and “white lists”. Signatures of content filters should be updated on a daily basis
- Content filters should be used to block access to material that is considered inappropriate (for example, pornography)
- Policies as to what constitutes acceptable content may be determined by Management or Compliance rather than the IT Head specifically.

3.5.2 Router / Core Network Switch

- Implement Access Control Lists (ACLs) to limit communications between networks
- All network ports listed in the switch configuration are to be configured with a description of the device connected
- Devices are to be patched and maintained in response to operating system and product alerts issued by the respective vendors
- Disable the use of VLAN trunking configuration on switch ports that do not require this configuration

3.6 Antivirus

- Antivirus gateways are implemented to monitor outgoing and incoming web and email traffic for suspicious activity that may be suggestive of the existence of a virus or other malware
- Network connections from workstations to the Internet should be blocked to prevent the spread and activation of malware