Mpee Finance Private Limited

Information Technology Policy

Table of Contents

Contents

Password Management Procedure

- Strict password parameters such as password complexity, minimum and maximum age, minimum length, number of bad logons, password history shall be configured & enforced for all users, including system/application administrators irrespective of the application/software.
- All system-level passwords (e.g., root, enable, NT administrator, application administration accounts, etc.) must be changed every 30 days.
- Hard-coded passwords in applications and scripts shall be changed every 30 days.
- The identity of a person requesting a password change/reset should be verified, irrespective of communication medium used.
- Users should be provided initially with a temporary password for all possible software that they are forced to change on the first system access; the initial password should be passed directly to the user after positive identification.
- Conveyance of passwords by unprotected (clear text) email messages or WhatsApp messages should be avoided. Users should acknowledge receipt of passwords.
- IT Team must ensure applications contain the following security precautions before procurement & deployment:
    - Should support authentication of individual users, not groups.
    - Issue a temporary password initially to the user after identifying him/her, and mandatorily forcing a password change upon first logon.
    - Ensure the software provides for some sort of role management, such that one user can't take over the functions of another without knowing the other's password.
    - Ability to enforce strict password parameters such as password complexity, minimum and maximum age, minimum length, number of bad logons and password history as specified in MPEE FIN 's Information and Cyber Security Policy.

User Responsibilities

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every quarter.
- Here is a list of "don'ts":
    - Don't reveal a password over the phone to anyone
    - Don't reveal a password in an email message
    - Don't reveal a password to the boss/senior
    - Don't talk about a password in front of others

- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Do not store the password in any file, program, command list, procedure, macro, or script where it is susceptible to disclosure or use by anyone other than its owner.
- Do not write passwords down and store them anywhere in your office.
- Do not re-use passwords.
- Do not use the same password for Mpee accounts as for other non- Mpee access (e.g., personal accounts, option trading, benefits, etc.). As much as possible, don't use the same password for various Mpee fin access needs.
- Do not share Mpee passwords with anyone, including administrators, assistants or secretaries. All passwords are to be treated as sensitive, confidential Mpee information.
- Do not use the "Remember Password" feature of browsers and applications (e.g., Yahoo mail, etc.)
- Do not insert passwords into email messages or other forms of electronic communication, including ticketing software.

- If an account or password is suspected to have been compromised, report the incident to the CTO and change all related passwords.
- If public systems are used to access Mpee information assets, then password used to access the resource has to be changed when the user returns to Mpee trusted network.
- If someone demands a password, refer them to this document, or report to the ISRM Team.

Maximum Password Age

This setting ensures how long a password will be active before it becomes mandatory for the users to change it.

Maximum Password Age is of 90 days for the following:

- Servers
- Production Servers and Applications
- Access Control Systems
- Firewalls and other Network Devices
- Domain Users
- Email Users

- Application Users
- WiFi Access

Minimum Password Age

The Minimum password age policy setting determines the period of time (in days) that a password must be used before the user can change it. The minimum password age must be less than the Maximum password age.

As per the password policy of MPEE, minimum password age is set 7 days.

Maximum Lockout Threshold

This setting ensures number of tries that a user can get to enter an incorrect password before account locked out.

Setting should be of ------- attempts for the following:

- Servers
- Production Servers and Applications
- Access Control Systems
- Firewalls and other Network Devices
- Domain Users
- Email Users
- Application Users

Password Strength

Password strength is a measure of the effectiveness of a password against guessing or brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability.

To ensure a good password strength, the password shall consist of:

- Minimum 8 characters
- Combination of alphanumeric characters
- 1 special character

Password History

This setting determines the number of unique new passwords that must be associated with a user account before an old password can be reused. Password reuse is an important concern in any organization. The longer the same password is used for a particular account, the greater the chance that an attacker will be able to determine the password through brute force attacks.

Users are not allowed to re-use last 3 passwords.

Anti-Virus

Installation of virus and malicious software protection software

- A centralized anti-virus server engine is setup on the cloud which shall automatically push updates to all client software agents installed on end-point devices as soon as they are connected to Mpee corporate network or internet.
- Mpee IT Administrator should ensure that Anti-Virus software is installed in all possible entry points (Servers, Laptops, etc.) of viruses and Malicious Software. He/she should also ensure that they are installed with the latest version of the Anti - Virus Software by checking the endpoints on a sample basis once in a month.

Update of virus signature files

- These are the files, which contain the data on virus signatures. The update of anti-virus can be automated using software or can be done manually.
- **Automatic Update**
  - The anti-virus server connected to the Internet checks the vendor site at a scheduled time for any new virus updates.
  - If there is any update, it should download it and push the update to the server.
  - From the server, an operating system job should be scheduled in the network server for pushing these signature file updates onto servers/MPEE computers/laptop computers/network nodes connected.
  - This job should be scheduled to run immediately after copying the signature files on the central host computers.

- **Manual update**
  - A system connected to the Internet checks the vendor/ supplier site at a scheduled time for any new virus updates.
  - If there is any update, it should download and it should notify the IT Administrator/ CTO about the new update.
  - The IT Administrator / CTO should then update the servers / desktops / laptop computers with the latest virus signature files.

Anti-virus software upgrades

- The upgrades are the newer versions of the anti-virus software. It is the responsibility of the CTO to procure and provide newer versions/engines of Anti-virus programs in regular and timely manner and ensure a quick rollout.

Review of logs

- Server Administrators/ IT Administrator should check the logs every 15 days (2nd and 4th Monday of every month) to review whether the desktops / laptop computers / servers were infected with viruses. He should report to the CTO every month about virus incidents detected and removed during that month.
- IT Administrator should review the anti-virus software activity/logs, especially to check whether the users are running the Anti-Virus system regularly on their desktop/ laptop computers (in case the user has the option to stop the scan).
- IT Administrator should also check all the servers/ desktops/ laptops on a sample basis every month to ensure that they are updated with latest version.

User Awareness

- Users shall be educated to communicate any issues regarding connectivity to anti-virus server engine or potential compromise of device with viruses or malware to the IT team.
- End-users shall connect their firm-provided devices to the corporate network as frequently as possible or at least once every quarter to ensure timely download of all anti-virus patches and update of their end-point software firmware.

Privilege Management

Privilege – Job function Matrix

- IT administrators or CTO along with the Department Heads should identify all the privileges associated with all Operating System, Business applications, Databases and Network elements used within individual businesses.
- These privileges should then be mapped with the job functions/ roles of the personnel involved in Mpee operations to develop and document Privilege – Job Function Matrix Wherever applicable, application roles should be created for each of the corresponding job function in the business.
- The review exercise should also be carried out whenever an Application or Operating System or a Database or network equipment is to be used for the first time.
- Privilege – Job function Matrix should be modified by IT administrator or CTO in the following scenarios:
    - When an Application, Operating System, Database or network equipment undergoes a major change or new module or functionality is added.
    - A new job function or role is created
    - Job Function or Role is changed.
- Privilege – Job Function Matrix should be approved by CTO before implementation.

Granting Access Rights

- Access Rights are granted to users on two occasions. One is during the creation of user account and when a user requests for additional access due to changes in job function or changes in responsibilities. Users assigned high privileges for special purposes should be required to use a different user identity for normal business use (e.g. "System Administrator" login is not to be used for running the application).
- When a new user is created, the access should be granted as per the request of the HR after verifying the approval and authorization from Department Head. Once the access rights are granted then record should be updated by the person who creates the user.
- If a user requires additional access rights/ privileges, then he/she should send an email along with valid business need and approval from Department Head to IT team for the same. Department Heads should ensure that the additional access rights/ privileges are absolutely required for performing his job functions.
- Any access that is not explicitly authorised is forbidden.
- Once the access privileges are granted then record should be updated by the person who

granted additional privileges.

- IT team should ensure that all devices connecting to the Mpee network should be mapped to respective employee/guest names

Review of Access Rights

- While the Department team leaders should review the access granted to his/her department personnel every 6 months and ensure that unauthorized access rights have not been accidentally granted to anyone, the CTO should review the list of users in various information systems along with their access privileges on an annual basis. He should verify, via sampling, in the information systems whether the privileges granted to the user is as per what is approved and documented.
- The Department Head who approved the additional access/privilege for their application should ensure that the same is revoked when the business purpose of the access ceases to exist. An email notification should be sent to IT team for the same.
- IT Team should verify whether the privileges are removed when the expiry date of them is over.
- IT Team should also check whether any additional privileges are obtained in an un-authorized manner and report any deviations to the Department Head/ CTO respectively.
- Review of Access Control List of the network shared drive/ folders for servers should be done by respective data centre team on half yearly basis and exceptions shared with the CTO.
- IT administrator or CTO should set appropriate access controls on all necessary file shares.
- All users of the information systems will be responsible for taking due care in the use and operation of the information systems through their user ID. Users will be held responsible for any activity carried out through their User IDs.

Remote Access to the Network

- Remote administration connections are considered to have a high degree of information security risk and therefore remote access to network should be approved by the IT Team.
- For third party users (consultants, auditors, vendors, etc.), remote connections are not allowed. They need to come to Mpee office or access the Mpee environment through a scheduled and approved Web-Ex session.
- All remote access connections to the network should be logged. These logs should be monitored by the IT Administrator on monthly basis.
- A timeout should be used to automatically disconnect all idle sessions for more than 5 minutes;
- Passwords should be regularly changed and accounts should lock after a number of unsuccessful attempts to log in (in accordance with organizational password policy)
- In case of any issues or incidents related to remote access the user should immediately report the same to the Chief Technology Officer (CTO).

Exception

- The access control procedure may not be followed during crisis or emergency situation, provided same is authorized by Chief Executive Officer (CEO) or Chief Operations Officer (COO).
- In case of an emergency situation (like fire, earthquake etc.), all physical access controls may be disabled for facilitating evacuation.

Sensitive System Isolation

- All sensitive systems should be identified. Unless specifically mentioned, systems processing 'confidential' and 'highly sensitive' information should be treated as sensitive systems.

Handling sensitive systems

- All sensitive systems should have a dedicated (isolated) computing environment.
- The following points should be considered for sensitive system isolation:
    - The sensitivity of an application system should be explicitly identified and documented by the application owner.
    - When a sensitive application is to run in a shared environment, the application systems with which it will share resources and the corresponding risks should be identified and accepted by the owner of the sensitive application.

Management of Network

Network Control

The following steps are taken to establish and maintain controls over the security of the Mpee network:

- A firewall is installed to protect against unauthorized access attempts over the internet;
- Access to unauthorized sites is managed through Access Control Lists;
- Any user requiring access to restricted sites for a business need shall be given access post review from the IT Team/CTO
- All Mpee employees are appropriately authenticated prior to accessing the Mpee network, and internet based applications;

Security of Network Services

The following steps are taken towards security of network services:

- E-mail traffic should be encrypted;
- Standard SSL or HTTPS protocols should be deployed while accessing IT applications over the internet / through browser (where applicable);
- Remote access is configured through VPN client. Mpee users must use the VPN to access Mpee network basis their credentials. Remote accesses to the Mpee network are controlled through user authentication & MFA mechanisms such as:
    - Refer - Access Management Procedure;
- The switch and firewall configuration is backed up by the IT team on a monthly basis;

Security of Operating Systems

- Mpee IT team shall be notified of all the patches and updates released by OEM over the email.
- The patches and updates shall be reviewed and implemented on a monthly basis by the IT Team.

Internet Access

Internet access for employees and contractors is granted based on approval of the Mpee management.

Internal Access Procedures

- All machines on the LAN shall authenticate to the Firewall before gaining access to the Internet.
- Access to internet shall be processed through a content filter and only appropriate categories that are required for the business shall be allowed.

- All Internet traffic shall be scanned for Virus, Trojans and malicious code by the local anti-virus (AV) agent installed on all the user systems.

Internet Access Guidelines for Users

Internet users are prohibited from transmitting, displaying or storing material that is fraudulent, obsessive, pornographic, profane, threatening, racially or sexually harassing or otherwise unlawful or improper or even visiting sites known to contain such material. Employees misusing given privileges will be subject to close monitoring of their computer system/assets and disciplinary action leading to but not limited to termination of employment or legal prosecution.

Examples of inappropriate employee Internet usage include but not limited to the following:

- Conducting or participating in illegal activities including gambling.
- Accessing or downloading pornographic material.
- Solicitations for any purpose which are not expressly approved by company management
- Revealing or publicizing proprietary or confidential/highly confidential information
- Making or posting indecent remarks
- Uploading or downloading commercial software in violation of its copyright
- Uploading or mailing of company's proprietary information without the consent of the information owner.
- Enter into contractual agreements via the Internet; e.g. enter into binding contracts on behalf of the company.
- Attempt to gain illegal access to remote systems on the Internet
- Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on the company network or systems.

Logging and Review

- Internet access logs derived from the Firewall shall be maintained for a period of 30 days. Logs of web sites visited, files downloaded, and time spent on the Internet, and related information shall be maintained.
- Access to the log files shall be restricted only to authorized Mpee personnel from the IT team.
- Privileged user accounts shall be logged and monitored to prevent falsification of logs.
- All incidents or anomalies shall be reported as per the Incident Handling defined in the Incident Management procedure document.

Firewall Security

Guidelines for Firewall Implementation

- Any unused networking protocols shall be removed from the firewall operating system build.
- Any unused network services or applications shall be removed or disabled as unused applications are often used to attack the firewall system. Any unused/unnecessary user or system accounts shall be removed or disabled.
- All relevant operating system patches and hot fixes shall be applied regularly (manually). The patches and hot fixes must be tested & confirmed prior to installation on production system.

Below are the guidelines for good firewall practices include but not limited to:

- Using a rule set that disallows all inbound and outbound traffic that is not specifically allowed
- Using NAT and split DNS to hide internal system names and addresses from external networks
- Using proxy connections for outbound HTTP connections and filtering malicious code
- Hardening the firewall by removing all unnecessary services and appropriately patching, enhancing, and maintaining all software on the firewall unit
- Restricting network mapping capabilities through the firewall, primarily by blocking inbound ICMP (Internet Control Messaging Protocol) traffic
- Backing up firewalls to internal media and not backing up the firewall to servers on protected networks
- Logging activity, with daily administrator review and limiting administrative access to few individuals
- Using security monitoring devices and practices to monitor actions on the firewall and to monitor communications allowed through the firewall
- Administering the firewall using encrypted communications and strong authentication, accessing the firewall only from secure devices, and monitoring all administrative access
- Making changes only through well-administered change control procedures

Backup of Firewall Configuration

Mpee shall take configuration back up of the Firewall. The configuration backup is performed on weekly basis and retained for a period of 90 days; the backup of logs shall be taken on a monthly basis and retained for a period of 90 days.

Wireless Security

- Shield the area in which the wireless LAN operates to protect against stray emissions and signal interference.
- Monitor and respond to unauthorized wireless access points and clients.
- All wireless Access Points connected to the corporate network must be registered and approved by IT Team of Mpee. These Access Points need to be subjected to periodic penetration tests and audits.
- Updated inventory on all wireless Network Interface Cards used in corporate laptop or desktop computers shall be available.
- Mpee shall ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Mpee shall deny access to those wireless devices that do not have such a configuration and profile.
- Mpee shall ensure that all wireless access points are manageable using enterprise management tools.
- Mpee shall use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromise. In addition to WIDS, all wireless traffic should be monitored by a wired IDS as traffic passes into the wired network.
- Where a specific business need for wireless access has been identified, Mpee shall configure wireless access on client machines to allow access only to authorized wireless networks.
- Mpee shall regularly scan for unauthorized or misconfigured wireless infrastructure devices, using techniques such as "war driving" to identify access points and client accepting peer-to-peer connections. Such unauthorized or misconfigured device should be removed from the network, or have their configurations altered so that they comply with the security requirements of the organization.
- Mpee shall ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection. Mpee shall ensure wireless networks use authentication protocols such as EAP/TLS or PEAP, which provide credential protection and mutual authentication.
- Mpee shall ensure wireless clients use strong, authentication credentials to mitigate the risk of unauthorized access from compromised credentials.