Date:20th June 2023

NOTE

Sub: Security Policy for Controlled Access of Maha-Metro IT system.

As per the directives given by top management of Maha-Metro for IT security of Maha-Metro systems, a draft for controlled access to IT systems of Maha-Metro has been prepared. Industrial Security Manual 2020 of Intelligence Bureau, MHA and counter measures of CERT-In has been referred to prepared it. This draft covers all area of IT in Maha-Metro to ensure its security and controlled access. Implementation of these policies will ensure standard industrial security practices.

It is reviewed and approved by NMRP/Team. It is put up here for final approval.

Encls: As Above (10 pages)

20/6/23
(Kiran Sonkusale)
Jt.GM/IT
PMRP

IT Security policy is put up for approval.

(Rajeev Kumar)
ED/IT-AFC
23/6/23.

(Vinod Kumar)
Dir(S&O)
Approved
22/6/23

Security Policy for Controlled Access of IT system in Maha-Metro

Maha-Metro Rail Corporation Limited has a large IT network which demands a policy to govern it to ensure proper functioning of all systems. Such a policy would necessitate consistency thus facilitating efficiency, a feature that is greatly desired. It would bring in discipline and accountability to the system, increasing reliability and ensuring sustainability.

Salient Features

The Maha-Metro Rail Corporation Limited IT policy aims to:

- Protect the organization, its employees, its customers, and also vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information; &
- Ensure the availability of information systems.

In brief, it consists of the following features:

- The procedures that must be followed by the organization to ensure that data integrity is maintained.
- The procedures that must be followed in the case of a breach of security or any other threat.
- The responsibilities of individuals of the organization, with respect to the IT sector, including but not limited to safe practices, the chain of command for reporting breaches, access controls.

Index

A. Introduction

This Policy Document encompasses all aspects of security surrounding confidential Maharashtra Metro Rail Corporation Limited information and must be distributed to all employees. All employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

B. Scope

This policy applies to all Councilors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Maharashtra Metro Rail Corporation Limited who have access to Maha Metro's information systems or IT equipment's.

C. Policy Compliance

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance. The appropriate course of disciplinary action would be decided post mutual consensus between the Administration Head, IT Head, Finance Head, and the HR Head, depending on the severity of the violation.

If you do not understand the implications of this policy or how it may apply, you may seek advice from IT Department.

D. Version

MM.IT.Policy@2023-Version.1.0

Chapter 1. Computers and IT Hardware

1. Each installation should have complete details and inventory list on number of PCs, workstations, monitors, laptops, scanners, printers, digital audio tapes CDs/DVDs, pen drives, external hard drive etc.
2. Three levels of basic access control measures that is (i) BIOS Passwords (ii) OS Password and (iii) Screen Saver Password must be implemented in all computers. Passwords should be strong alpha-numeric having special characters and should be changed periodically. For highly sensitive systems smart cards or biometrics devices (fingerprints or iris, etc.) should be used.
3. Auto play, auto run and remember password options to be disabled in all computers.
4. It should be ensured that only approved USB drives/pen drives are used with proper logs being maintained. All permitted USB devices are properly formatted/sanitized after every use.
5. Regular backup of data should be taken to avoid loss from incidents like malware infections, hardware & software failures. The organization should have data backup policy and a disaster recovery plan.
6. OS, anti-virus, intrusion detection & other applications software should be regularly updated utilizing propriety software complying with intellectual property rights and licensing agreements.
7. Organizations following concepts like Bring Your Own Device (BYOD), Bring Your Own Technology (BYOT), Bring Your Personal Computers (BYOPC) should be discontinued as such policies as it brings significant risks and data breaches.
8. Under any circumstances, secondary storage media (hard disk/solid state disk in computer, printer, photo state machine etc.) should not be handed over to third party maintenance outside the installation. No equipment (computer, photo state machine, printer etc.) with secondary storage media should be sent outside installation for maintenance/condemnation process, etc.
9. Mobiles phones should not be connected to the official computers/laptops for any requirement including charging. It could result in transfer of malware to the system inadvertently.

Chapter 2. Network, Servers & Internet

1. Inventory of connected devices, systems, monitors on LAN/WAN, Internet and other dedicated network of the organization should be maintained and updated periodically.
2. Local or Wide Area Networks should be controlled such that only authorized users can gain access.
3. Organizations should have copies of documentation describing logical & physical layout of the network.
4. Tools for network managements, monitoring packages and devices should be available to network administrators. Network events should be automatically logged by the network operating system. The log should be periodically reviewed for unauthorized activities.
5. The internet connection should be provided only on standalone computers through own gateways. Such computers are to be physically isolated from the main information system. All unnecessary logical ports on the internet sever should be closed.
6. The physical components of the network such as wires, servers, switches, routers, encryptors and other communication devices and links must be protected, installed in a structured manner and well labelled.
7. AMC firms must be registered and only authorized staff post police verification should carry out maintenance trouble shooting repair/replacement and expansion work on the system.
8. There should only be official Computer Storage Media (CSM) and record of its usage must be maintained. Storage media no longer required should be disposed of securely & safely as per laid down procedures and record of such disposal/destruction to be maintained.
9. Disposal procedures of all ICT assets and equipment should be centrally managed and coordinated by the relevant sections. All hardware slated for disposal by any means must be fully destroyed/wiped clean of all data. Owner of the concerned section should assume responsibility for decommissioning the equipment by deleting all files, licensed programs, and applications using a pre-approved disk-sanitizer.
10. Ensure that media that is no longer required operationally (e.g. due to expiry, surplus, damage or wear), should be disposed off securely. Storage devices (hard disks, pen drives, CDs/DVDs, etc.) containing sensitive information should be destroyed beyond recovery of data (e.g. physical shredding, disintegration, pulverisation, or incineration).
11. Equipment should be protected from environment hazards (like flooding, lightening, fire, earthquake etc.), power failure and failures in supporting utilities and from other disruptions.
12. The organization should use Govt./corporate email domains. Use of Gmail, Yahoo and other such services, where servers are not located in India must be avoided. The email server of corporate email domains ideally should be located in India with adequate email server security and log trails. For reference installation may refer to 'National Email Policy' (Gazette Notification dated February 18, 2015)
13. There may be smart card/biometric based log in/out system for operators so as to maintain an accurate log record.
14. The network system security should cover essentials like firewall security, physical access security, password security, security settings and user rights etc. Apart from general IT control, adequate application controls measures should be placed for protection of standing data and master files, processing and input/output of transactions in the system.
15. The organization should have clear, documented operating procedures for all computer systems to ensure their correct, secure operation like system restart & recovery procedures,

instructions for handling errors or other exceptional conditions and details of support contacts for trouble shooting.

16. Server rooms operations and control rooms should have common physical access controls like biometrics access, locked doors, CCTV, intruder alarms and security guard cover. Smoke and fire detectors and associated alarm system to be fully functional in such locations (preferably under AMC).
17. If corporate network is connected to Internet, a firewall should be constructed to keep control of traffic between the two. Firewalls to allow only specific internet services and should provide services such as logging, authentication, packet filtering and encryption.
18. An appropriate authentication mechanism may be used to control access by remote users. Automatic equipment identification may be considered as a means to connect from specific locations and equipment. During long remote access sessions, periodic re-authentication method should be put in place to confirm that the person using remote access is authorized to do so. Whenever feasible.
19. Implement mutual authentication, so that a remote access user can verify the legitimacy or a remote access server before providing authentication credentials to it. All remote access activity should be closely monitored and a record (date, users, duration, type of activity etc.) of such access should be maintained.
20. Data exchanges between the sensitive systems and remote accessing system should be always in offline mode and should adhere to security guidelines of transferring data from internet-connected computer to non-internet connected system.
21. An action taken/compliance report should be prepared on the last Third Party Security Audit.
22. For installation with large number of ICT assets, it should have a full-fledged Security Operation Centre (SOC). SOC and Network Operation Centre (NOC) should be manned separately. A dedicated team should be detailed for analyzing and reporting the various security events/logs noticed in the SOC.
23. Without hardening and security patch updating (testing, wherever feasible), no new equipment should be connected to the live environment.
24. Any addition or removal of network elements should be properly recorded and the network diagrams should be accordingly updated.

Chapter 3. Social Networking Sites

1. Employees should not use organizational email addresses on social networking sites (SNS).
2. Access of SNS/non-officials web-portal should be limited to extent of organization's benefits and which must have perceived benefits for organization should be permitted with limited functionality.
3. Organizations having internal social networking platforms should have adequate information security measures.
4. Organizational account on social network site should not show names with job titles, email addresses, professional background and expertise and associations of executives and members.
5. Employees posted in sensitive sections, handling sensitive projects should not be allowed to post about their jobs and projects on Social Media platforms, messenger apps, etc. Non-Disclosure Agreement (NDA) may be made to bind such employees.

Chapter 4. IT and Cybersecurity

1. CERT-In guidelines hosted on its website for email usage, server security, Intrusion Detection System, Anti-virus policy, system security, Security of computers connected to networks etc. should be followed.
2. Vulnerability notes and advisories regularly hosted on CERT-In website must be taken into account by the installation computer security and IT team and their AMC support partners. CISO should be responsible for implementation of the same.
3. Installations should have Computers and Information Security Policy conforming to CERT-In and NIC directives, policy & guidelines (in addition to their own corporate/sector guidelines) Staff awareness programs should be structured so as to achieve full compliance of such policy.
4. No organization related data should be given to visitor without the prior written approval of competent authority (head of the plant/installation). However, under any circumstances, classified information would never be shared with the visitor.
5. Visitors should not be allowed to connect their devices to any of the ICT networks/ systems.
6. All visitor electronics should be checked out individually as per extent procedure followed in Check-in/Check-out for Laptop. Computer and related equipment.
7. There should be clearly defined roles and reasonability policy for handling managing, accessing ICT assets of installation Suitable measures on breach of cyber security should be defined in such policy and all concerned employees should be made aware of such policy.
8. A clear Non-Disclosure Agreement (NDA) should be made with outsourced partners, vendors, etc. The NDA should bind both the vendor organization as well as the employees of the vendor organization so that even the employees of the organization leaves, he should be bounded by NDA.
9. Periodic audit and Vulnerability Assessment and Penetration Testing (VAPT) of ICT assets of installation be done from empaneled ICT auditors.
10. There should be a separate full time CISO and staff, suitably qualified to ensure cyber security. An IT organizational chart to be available.

Chapter 5. General Security instructions

1. Install and maintain updated anti-virus and anti-spyware software at desktop level.
2. Scan computer system with updated anti-virus for possible infections and disinfect the same.
3. Install and maintain personal desktop firewall.
4. Check for the suspicious network activities of infected computer system mentioned in list and disinfect the same if found.
5. Use only genuine software.
6. Keep up-to-date patches and fixes on the operating system and application software.
7. Exercise caution while opening email attachments.

References:

1. Industrial security Manual 2020, IB, Ministry Home Affairs.
2. Counter measures and security best practices given by CERT-In