MICL CYBER-SECURITY POLICY

1. *Policy Brief*

Cybersecurity is the practice of protecting electronic information by mitigating information risks and vulnerabilities. Information risks can include unauthorized access, use, disclosure, interception, or data destruction. MICL recognizes that, in this complex digital world, a single security breach can have far-reaching consequences, including financial loss and loss of customer trust. The objective of this policy is to ensure proper access to and usage of IT resources and prevent their misuse by the users.

2. *Purpose:*

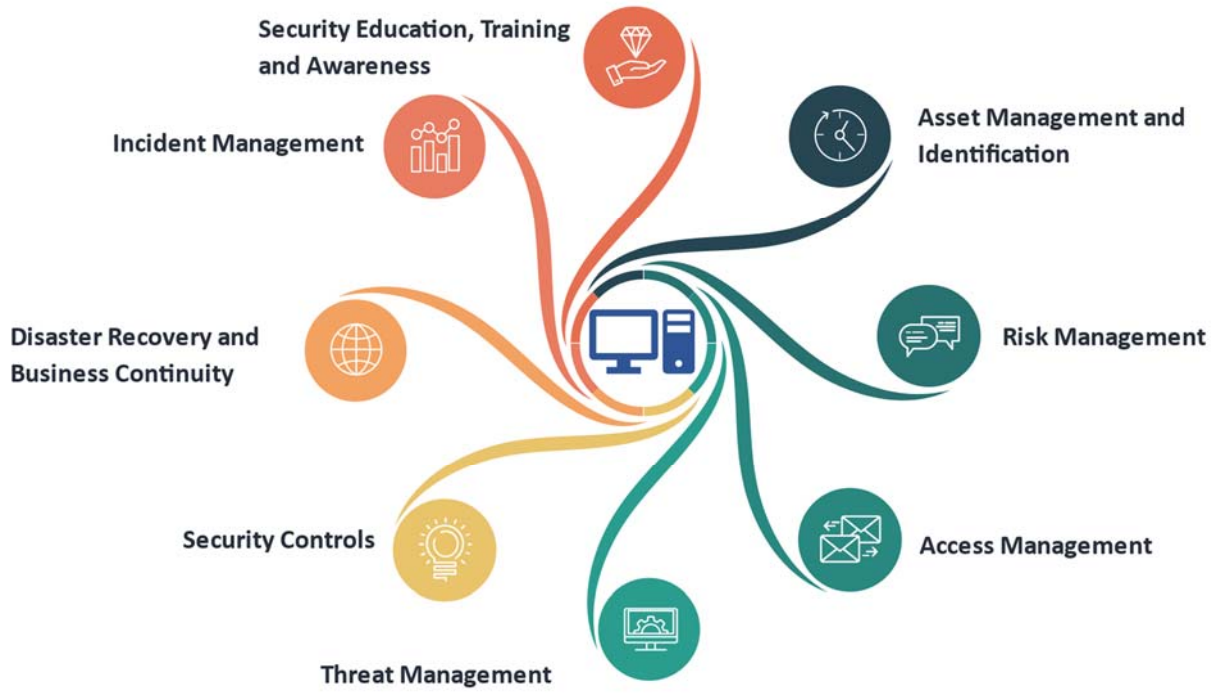
The purpose of the policy is to protect information and information infrastructure from cyber incidents through a combination of processes, guidelines, technology and cooperation. This policy governs the usage of IT Resources from an end user's perspective.

This Policy defines what we want to protect and what we expect of our system users. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords and describes how we will monitor the effectiveness of our security measures.

3. *Scope and Applicability:*

This policy applies to MICL including its Associate Companies, Subsidiaries, and Joint Venture. MICL also expects independent contractors and all involved in the value chain to uphold the principles ofthis Policy and urges them to adopt similar policies within their own businesses. It is mandatory for all users to adhere to the provisions of this policy.

4. *Elements of Cybersecurity*



5. *Policy Statement*

- MICL will protect all its stakeholders' interests by ensuring confidentiality, Integrity and continuous availability of information and information systems under its control which includes, but is not limited to electronic, print information etc., on servers, workstations, laptops, networking and communication devices, tapes, CDs, and information printed or written on paper or transmitted by any medium.
- MICL will develop and deploy effective systems and procedures for 1) Asset Management and Identification 2) Risk Management 3) Access Management 4) Threat Management 5) Security Controls 6) Disaster Recovery and Business Continuity 7) Incident Management and 8) Security Education, Training and Awareness.
- MICL is committed to comply with all legal, regulatory, and contractual security obligations as may be applicable in cyberspace.
- MICL shall evaluate the business risk in information security perspective, prevent and reduce the risks to the maximum possible extent to avoid any undesired effects on business and Customers.

- MICL shall protect all Information from unauthorized access, use, disclosure, modification, disposal, or impairment whether intentional or unintentional, through appropriate technical and organizational security measures.

- MICL is committed to provide a virus free network and all Information processing systems will be auto updated with latest security patches from the manufacturer and loaded with an approved antivirus system.

- MICL shall provide framework to manage and handle security breaches, violations and business disruptions.

- MICL shall ensure continuity of critical operations in line with business and contractual requirements.

- A comprehensive backup procedure will be implemented to protect the business transactions. Backup tapes are to be verified by restoring the data for integrity as per SOP. Data owners and system owners are responsible for identifying the type(s) of data their systems generate, process, collect, or store. Once identified, appropriate backup and recovery measures should be designed, and an appropriate record retention/destruction schedule chosen.

- Only authorized and licensed software will be allowed to be installed on corporate systems.

- Company network will be always protected from the Internet through a firewall.

- All third-party partners dealing with MICL who use IT information assets will be asked to sign a non-Disclosure agreement (NDA)

- All servers to be located in a secured area with restricted access.

- All information assets used in production will have either warranty or a support contract from the authorized vendor/ partner.

- MICL is fully aware of maintaining the data privacy of its customers and treats it as its own data taking all necessary security and privacy protection. The information obtained by MICL from the customer for the purpose of business will be used only for the purpose it was sought such as processing applications and transactions, maintaining your account in the system, responding to your queries, etc.

- Disposal of media, any information processing systems will follow the E-waste policy.

- All changes in the information processing system will be managed through the change control process

6. Policy - Concepts & Guidelines

i. Confidentiality

The assurance that sensitive information remains private and is not visible to an eavesdropper. Confidentiality is critical to total data security. Encrypting data by using digital certificates and Secure Socket Layer (SSL) or virtual private network (VPN) connection helps ensure confidentiality when transmitting data across untrusted networks.

ii. Auditing security activities

Monitoring security-relevant events to provide a log of both successful and unsuccessful (denied) access. Successful access records tells who is doing what on your systems. Unsuccessful (denied) access records tells either that someone is attempting to break your security or that someone is having difficulty accessing your system.

iii. Integrity:

Integrity would imply the assurance that the arriving information is the same as what was sent out. Understanding integrity requires to understand the concepts of data integrity and system integrity.

a) Data integrity: Data is protected from unauthorized changes or tampering. Data integrity defends against the security risk of manipulation, in which someone intercepts and changes information to which he or she is not authorized. In addition to protecting data that is stored within our network, we might need additional security to ensure data integrity when data enters our system from untrusted sources. When data that enters our system comes from a public network, we need security methods so that we can perform the following tasks: –

- Protect the data from being sniffed and interpreted, typically by encrypting it.
- Ensure that the transmission has not been altered (data integrity).
- Prove that the transmission occurred (nonrepudiation). In the future, you might need the electronic equivalent of registered or certified mail.

b) System integrity: Our system provides consistent and expected results with expected performance. For the OS operating system, system integrity is the most commonly overlooked component of security because it is a fundamental part of OS architecture.

iv. Asset Management & Identification

a) One of the most critical aspects of any strong cybersecurity posture is knowing exactly what assets are a part of MICL's network. Identifying all of the devices and software platforms that are linked to your network is the first step in maintaining security hygiene and closing any gaps in your cybersecurity posture.

b) **Device Identification:** The devices include Printers, Mobile Devices (tablets, smartphones, etc.), Workstations, Network Hardware, Servers, Third-Party Systems (those assets that exist in all of your third-party partners' networks that may affect your cybersecurity hygiene).

c) **Platform Identification:** The most common platforms are Mac, Windows, and Linux, but some devices may run other platforms as well. Knowing which platforms are running on each device is a key part of managing your IT assets in the long term, as it helps you know which devices need patching for recently-revealed security vulnerabilities.

v. Risk Management

a) A risk assessment's purpose is to identify the risks and likely impacts, if any given threat is successful. A critical step in a risk assessment is to determine risk and impact as well as analyze the control environment.

b) Steps involved in Risk Management include 1) Characterize the System 2) Identify Threats 3) Determine Risk and Impact 4) Analyze the Control Environment 5) Determine the severity and likelihood rating and 6) Calculate the risk rating

vi. Access Management

a. All devices on the network of MICL should not be accessible without proper authentication. Authentication for access of MICL's computer networks shall be obtained after following the due process and procedure as prescribed by the IT team.

b. Access Controls are applicable to Network Access, Wireless Access, Wired Access and Physical Access.

c. Using the principle of least privilege is important for minimizing the company's exposure. This principle implies that the access privileges is restricted, based on the role of the user, to the absolute minimum necessary for them to fulfill their role.

d. The assurance or verification that the resource (human or machine) at the other end of the session really is what it claims to be. Solid authentication defends a system against the security risk of impersonation, in which a sender or receiver uses a false identity to access a system. Traditionally, systems have used passwords and user names for authentication; digital certificates can provide a more secure method of authentication while offering other security benefits as well. When system is linked to a public network like the Internet, user authentication takes on new dimensions. An important difference between the Internet and intranet is the ability to trust the identity of a user who signs on. Consequently, one should consider seriously the idea of using stronger authentication methods than traditional user name and password logon procedures provide. Authenticated users might have different types of permissions based on their authorization levels.

vii. Authorization

Authorization implies assurance that the person/computer at the other end of the session has permission to carry out the access authentication request.

viii. Threat Management

a) Threat Management is the process of identifying, assessing and addressing the potential weak points in our network infrastructure.

b) This involves three key procedures : 1) Penetration Testing 2) Vulnerability Management and 3) Patch Management

ix. Security Controls

a) Security Controls encompasses a range of administrative, physical, and technical controls that are used by your organization to prevent illicit access to sensitive information.

b) Administrative controls are a list of “Do’s and Don’ts” for employees to follow when accessing or using sensitive data.

c) Physical security references the various means you use to protect the physical assets on your network from being accessed by unauthorized personnel.

d) Technical security controls are all of the specific security measures used to protect your data. There are innumerable specific technical security controls that MICL may use. These include 1) Perimeter / Network Security – measures such as firewalls, traffic routing solutions 2) Multi-factor Authentication – two or more criteria to enable access to company resources 3) Segmentation of networks – the subdivision of some parts of network into discrete pieces that are isolated from everything else

4) Endpoint Security – Antivirus programs, host-based firewalls 5) Content Filtering – preventing employees from visiting specific websites from the workplace's network

x. Disaster Recovery and Business Continuity

a) Disaster Recovery and Business Continuity planning encompasses contingency plans to keep MICL's IT infrastructure up and running in the face of a major event that would normally prevent access.

b) This involves creation of backups of sensitive data on remote servers and copies of MICL network environment that runs our business' mission-critical applications that can be brought online in case of a catastrophic event.

xi. Security Incident Management Process

a) A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of data owned by MICL.

b) IT Department reserves the right to deactivate/remove any device from the network if it is deemedas a threat and can lead to a compromise of the system.

c) The steps involved are 1) Identification 2) Containment 3) Eradication 4) Recovery and 5) Corrective Actions / Lessons Learned

xii. Use of IT Devices

IT devices (Desktops, Printers, Scanners, Standalone PCs and other electronic devices connected to our network) issued by MICL to a user should be primarily used for official purposes and ina lawful and ethical manner.

xiii. E-mail Access from MICL's Network

a) E-mail service authorized by MICL should only be used for official correspondence.

b) All incoming SMTP e-mails will be scanned for spam and virus infection.

xiv. Access to Social Media Sites from MICL's Network:

a) Use of social networking sites by employees is governed by the IT Department. User should comply with all the applicable provisions under this policy while posting any data pertaining toMICL on social networking sites.

b) User should adhere to the "Terms of Use" of the relevant social media

platform/website, as well as copyright, privacy, defamation, discrimination, harassment and other applicable laws.

c) User should report any suspicious incident as soon as possible to the IT Department.

d) User should always use high security settings on social networking sites.

e) User should not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.

f) User should not disclose or use any confidential information obtained in their capacity as an employee/contractor of the organization.

g) User should not make any comment or post any material that might otherwise cause damageto the organization's reputation.

xv. Filtering and blocking of sites

a) IT Department may block content over the Internet which is in contravention of this policy and other applicable laws of the land in force which may pose a security threat to the network.

b) IT Department may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the network security and productivity of the users/organization.

xvi. Security Education, Training and Awareness

a) Awareness Trainings are conducted by the IT Head to all employees related to basics of cybersecurity. This includes dissemination of information relatd to Cyber-Security Policy and the various prevalent cyber threats on the net and the precautions to be taken therein.

7. Policy Compliance and Dissemination

a) It is the responsibility of all employees to adhere to the policy and the management has all rightsto take disciplinary action in case of its violation.

b) All employees of the organization are necessarily to be aware of the Information Security Policy ofthe organization.

c) Employees while operating from remote/outside organization network should strictly

connect viaVPN for accessing Applications and Corporate Network.

d) All employees should implement appropriate controls to ensure compliance with this policy by theirusers.

e) IT Department will ensure resolution of all incidents related to the security aspects of this policy bytheir users.

f) Users should not install any network/security device on the network without consultation with theImplementing Department

g) The IT Department should ensure that training and awareness programs on use of IT resources are organized at regular intervals. To ensure security awareness amongst Employee to enable them tomeet their security obligations. It Department should ensure proper dissemination of this policy. ITDepartment may use newsletters, banners, bulletin boards, corporate Websites and Intranet etc. to increase awareness about this policy amongst their users.

h) Orientation programs for new recruits should include a session on this policy.

8. Monitoring and Review:

MICL shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy. MICL for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on devices under intimation to the user. This includes items such as files, e-mails, and Internet history etc. Monitoring and review of this policy is governed by IT department. A periodic reporting mechanism to ensure the compliance of this policy should be established by the IT Department.

Any security incidents, security weaknesses and infringement of the policy actual or Suspected, are reported, investigated by the designated SOC team and appropriate corrective and preventive action initiated.

The Managing Director in consultation with the IT- Head is authorized to make modifications to thispolicy as and when deemed necessary and appropriate to ensure the ends of the policy being served.

9. Reporting and Remedy:

Any questions or concerns on matters concerning Cyber Security shall be reported to IT-Head, Corporate.

MICL assures through this policy that any Cyber Security Matters resulting from or caused by MICL's business activities shall be appropriately and adequately remedied in a time-boundmanner.