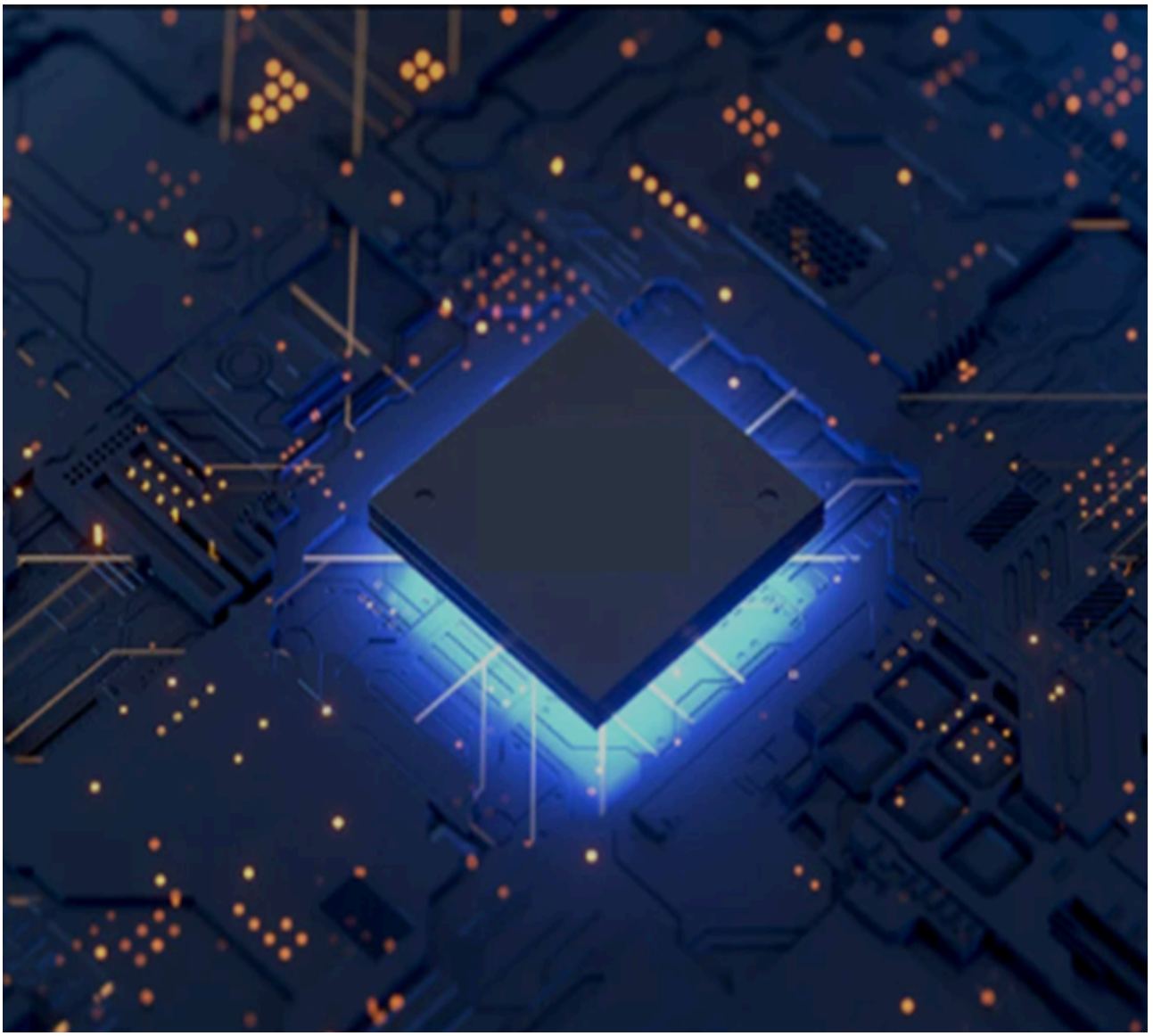


MIHUP COMMUNICATIONS PRIVATE LIMITED
ISO 27001:2022

Millennium City IT Park, Tower 2, 3A & 3B, 3rd Floor, DN-62, DN Block, Sector V, Salt Lake,, Kolkata - 700091, India

Document Details

Document:	INFORMATION SECURITY POLICY FRAMEWORK
Document Number:	MCPL/ISMS/L2/01/V2.0
Version:	2.0
Document Date:	01-June-2024
Prepared By:	CISO
Reviewed By:	ISSC
Approved By:	CEO
Classification Level:	Internal

Modification History

Sl. No.	Description of Change	Date of Change	Version No.
1	Initial Release	02-September-19	1.0
2	Re-Release with minor update	04-August-20	1.1
3	Reviewed but no changes	03-Ocotber-23	1.1
4	Updated as per the requirements of ISO 27001:2022	01-06-2024	2.0
5	Reviewed but no changes	04-11-2025	2.0

CONTENTS

1. INTRODUCTION

1.1 Objective

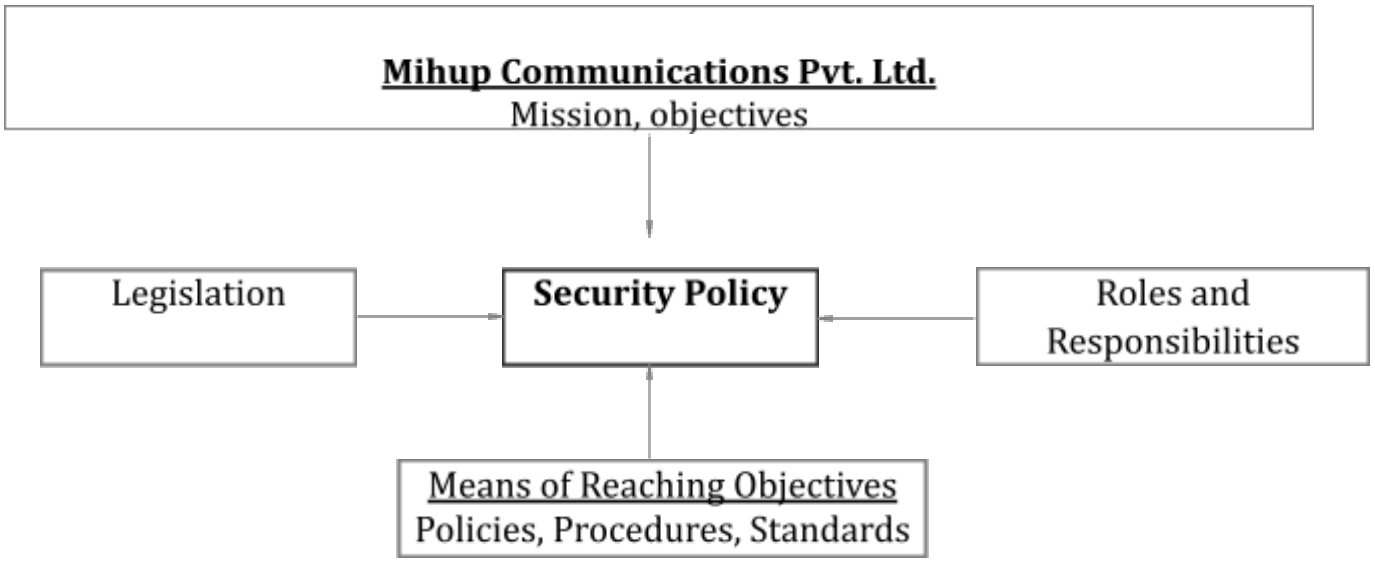
The objective of Mihup Communications Pvt. Ltd.'s information security is to ensure the business continuity of Mihup Communications Pvt. Ltd. and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

1.2 Policy

- The policy's goal is to protect the Mihup Communications Pvt. Ltd.'s informational assets against all internal, external, deliberate or accidental threats.
- The Chief Information Security Officer approves the Mihup Communications Pvt. Ltd. information security policy
- The security policy ensures that:
  - Information will be protected against any **unauthorized access;**
  - **Confidentiality** of Mihup Communications Pvt. Ltd. information will be assured;
  - **Integrity** of Mihup Communications Pvt. Ltd. information will be maintained;
  - **Availability** of Mihup Communications Pvt. Ltd.'s information for business processes will be maintained;
  - **Legislative and regulatory** requirements will be met;
  - **Business continuity plans** will be developed and maintained;
  - **Information security training** will be available for all employees;
  - **All actual or suspected Mihup Communications Pvt. Ltd. information security breaches** will be reported to the CISO and will be thoroughly investigated.
- Procedures exist to support the policy, including virus control measures, passwords and continuity plans.
- Business requirements for availability of Mihup Communications Pvt. Ltd. information and systems will be met.
- The CISO is responsible for maintaining the policy and providing support and advice during its implementation.

- ISIC & ISSC are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- Compliance with the Information Security Policy is mandatory.

ELEMENTS OF A SECURITY POLICY



This diagram presents a security policy as a document describing the mission, objectives and values of Mihup Communications Pvt. Ltd. The security policy reflects the values of Mihup Communications Pvt. Ltd. Accordingly, number of models is used depending on the Mihup Communications Pvt. Ltd.' line of business and objectives. Moreover, certain legal restrictions considered when elaborating security policies, such as stipulations of the data protection law, the access to information law, the law on the protection of personal information and electronic documents, etc. Defining the roles and responsibilities of staff members represents one of the most important aspects in getting all employees to work towards a common goal.

1.3 Goal of the Security Policy

Mihup Communications Pvt. Ltd. depends on information and information systems. The goal of the security policy is to set objectives for the organization as regards the protection of Mihup Communications Pvt. Ltd.'s informational assets. The security policy provides the basis for the implementation of security controls that reduce risks and system vulnerabilities. By clarifying the responsibilities of users and the measures, they adopt to protect Mihup Communications Pvt. Ltd.'s information and systems, Mihup Communications Pvt. Ltd. avoid serious losses or unauthorized disclosure. Moreover, the company's reputation is partly dependant on the manner in which it protects its Mihup Communications Pvt. Ltd. information and Mihup Communications Pvt. Ltd.'s information systems. Finally, a security policy can be useful as evidence in litigations, in client contract negotiations, during acquisition bids and for business relations in general. The management of Mihup Communications Pvt. Ltd. has initiated and continues to sustain a Mihup Communications Pvt. Ltd.'s information security effort thanks to the development of sound policies and procedures.

1.4 Security Management Framework

All policies and procedures included in this document are approved, supported and defended by the senior management of Mihup Communications Pvt. Ltd. As respect of the security policy is all-important to the corporation, Mihup Communications Pvt. Ltd.'s information entrusted to it be protected according to the critical value and sensitive nature of this Mihup Communications Pvt. Ltd. information. Security measures are taken, regardless of the storage media on which Mihup Communications Pvt. Ltd. information is saved, the systems used to process Mihup Communications Pvt. Ltd. information or the methods used to transfer Mihup Communications Pvt. Ltd. information. Information is protected according to its security classification, without regard to the phase of the Mihup Communications Pvt. Ltd.'s information life cycle in which it is found.

2. SCOPE

2.1 The Employees

Information security is a team effort. It requires the participation and support of all members of the organization who work with Mihup Communications Pvt. Ltd. information systems. Thus, each employee complies with the requirements of the Mihup Communications Pvt. Ltd.'s information security policy and it's attending documentation. Employees who deliberately or through negligence violate Mihup Communications Pvt. Ltd. information security policies will be subject to disciplinary action.

2.2 The Systems

This policy applies to all computers, networks, peripherals, applications and operating systems owned or operated by Mihup Communications Pvt. Ltd. The policy covers solely the Mihup Communications Pvt. Ltd.'s information handled by computers and networks.

3. ROLES AND RESPONSIBILITIES

3.1 Divisions that Manage Information Security

- ISIC' is responsible for establishing and maintaining Mihup Communications Pvt. Ltd.'s information security policies, standards, directives and organizational procedures.
- The Internal Audit Division ensures the compliance of Mihup Communications Pvt. Ltd.'s information technologies with policies, procedures and any applicable legislation.
- Investigating system hacking and other Mihup Communications Pvt. Ltd. information security incidents is the responsibility of the ISIC.
- Disciplinary action in response to violations of Mihup Communications Pvt. Ltd.'s information security regulations is the responsibility of local managers acting jointly with the Human Resources department.

3.2 Responsibility Categories

In order to coordinate security efforts, Mihup Communications Pvt. Ltd. has divided the responsibilities of its members into three categories.

i. User Responsibilities

Users are required to conscientiously familiarize themselves with all Mihup Communications Pvt. Ltd.'s information security policies, procedures, standards and applicable legislation. They fully understand these requirements and comply with them.

ii. Owner Responsibilities

- Owners of Mihup Communications Pvt. Ltd.'s informational assets are generally executives, managers or delegates of Mihup Communications Pvt. Ltd. who acquire, develop and maintain operational applications (decision support systems) which support decision-making and other organizational activities.
- *Each operational application has an appointed owner*.
- Owners indicate the classification that best reflects the sensitive nature, critical value and availability of each type of Mihup Communications Pvt. Ltd. information. The classification will, in turn, determine the level of user access.

iii. Responsibilities of Information Administrators - On premise applications

- ISIC members who are charged with the safekeeping of Mihup Communications Pvt. Ltd.'s information
- ISIC members are responsible for storing Mihup Communications Pvt. Ltd.'s information, implementing access control systems (to prevent unauthorized disclosure) and periodically running backups (to ensure critical Mihup Communications Pvt. Ltd. information is not lost).
- ISIC members are also required to develop, apply, maintain and revise the security measures defined by Mihup Communications Pvt. Ltd. information owners.

4. DEFINITIONS AND ABBREVIATIONS

IT: Information Technology

Malicious software: Program or part of a program intended to disrupt, alter or destroy all or part of the logic elements essential to the operation of a Mihup Communications Pvt. Ltd. information processing system. These programs can be divided into four classes: computer viruses, worms, Trojan horses and logic bombs.

5. INFORMATION SENSITIVITY AND CLASSIFICATION

5.1 Four (4) information classifications

- Information classification constitutes an important element of risk management, as it determines the needs, the priority and the degree of protection required for each type of Mihup Communications Pvt. Ltd. information.
- Mihup Communications Pvt. Ltd. has adopted an information classification structure that sees Mihup Communications Pvt. Ltd.'s information filed by category. This structure defines the appropriate level of protection for a given category and informs those responsible of any special measures or treatment required.
- All Mihup Communications Pvt. Ltd. information is integrated into one of the following four categories.
    - Restricted
    - Confidential
    - Internal
    - Public
- To ensure protection of Mihup Communications Pvt. Ltd.'s information, all users must familiarize themselves with the definition of each category as well as the measures required.

5.2 Information Labelling

- Mihup Communications Pvt. Ltd. has developed appropriate procedures for labelling and handling organization's information according to the classification structure it has adopted.
- Sensitive information, from inception to destruction, bears the appropriate Mihup Communications Pvt. Ltd. information classification designation.
- Labels appear in the header/footer of company documents.
- As most documents fall into the "Internal" category, it isn't necessary to put a label on this type of Mihup Communications Pvt. Ltd.'s information as it will be classified as such by default.

6. ORGANIZATION SECURITY

6.1 Disclosure to Third-Parties

- Information labelled other than "Restricted" be protected from disclosure to third parties.
- Third-party access to the Mihup Communications Pvt. Ltd.'s information may be permitted if it has been shown that this Mihup Communications Pvt. Ltd.'s information is needed to enable the third party to pursue the mandate it has been given by the organization. However, a non-disclosure agreement with Mihup Communications Pvt. Ltd. first be signed [Non-disclosure agreement/Confidentiality accord] and disclosure be expressly authorized by the Mihup Communications Pvt. Ltd. information's owner [List of the owners and types of Mihup Communications Pvt. Ltd. information which they control].
- Any loss or unauthorized or suspected disclosure of sensitive Mihup Communications Pvt. Ltd.'s information is reported immediately to the Mihup Communications Pvt. Ltd.'s information owner and to the Information Security Division.

6.2 Third-party requests for Information

- Unless an employee has been authorized by a Mihup Communications Pvt. Ltd.'s information owner to publicly disclose Mihup Communications Pvt. Ltd.'s information, all requests for Mihup Communications Pvt. Ltd. information concerning Mihup Communications Pvt. Ltd. be reported to CISO.

- Requests for questionnaires, financial reports, internal policy documents, procedures, surveys and interviews with personnel are covered by this policy.

6.3 Unauthorized Copying of Information

- It is forbidden for users to copy, without valid justification and authorization, the organization's information or software.
- Those responsible for the unauthorized forwarding of copied Mihup Communications Pvt. Ltd.'s information to third parties will be subject to disciplinary action.

6.4 External Disclosure of Security Information

Information regarding security measures for Mihup Communications Pvt. Ltd. information processing systems and networks is confidential and not be disclosed to unauthorized users, unless first approved by the Mihup Communications Pvt. Ltd.'s information security manager.

6.5 Information Handling and Transfer

Mihup Communications Pvt. Ltd. shall treat all information as valuable and shall care at all times. Following practiced shall be ensured:

- Confidentiality, Availability and Integrity must be maintained.
- Information must only be shared with those who have a legitimate need to see it.
- Lock sensitive/confidential information away, following 'Clear Desk' procedures.
- Only store the information authorized by IT team.
- Do not discuss sensitive/confidential issues in public.
- Report stolen or lost information as soon as possible.

All agreements entered into by Mihup Communications Pvt. Ltd. with Clients and other stakeholders shall provide, wherever necessary, for secure transmission of sensitive/critical information & software between them.

7. ADMINISTRATIVE SECURITY CONTROLS

7.1 Use of the Technological Resources of the Organization

- All employees who wish to use the Mihup Communications Pvt. Ltd.'s information processing systems should sign a compliance statement. In signing this statement, users indicate that they understand and accept to adhere to the policies and procedures of Mihup Communications Pvt. Ltd. as they relate to the use of computers and networks, including the instructions contained in the present policy.
- The information systems of Mihup Communications Pvt. Ltd. are to be used solely for professional purposes.
- Occasional personal use is permitted, if brief and without noticeable effect on productivity.
- It is forbidden to play games during working hours, as this negatively affects productivity and, as a result, profitability. Anyone found playing games will face disciplinary action.

7.2 Surveillance Rights

- Management reserves the right to monitor and inspect the organization's information systems at any time.
- These inspections can take place with or without the consent and presence of the employees involved.
- Information systems likely to be subjected to such inspection include the activity logs of users, hard drive files and email. However, printed documents, desk drawers and storage areas may also be subject to inspection.
- Inspections only are performed after having obtained the approval of the legal and security departments.
- CISO reserves the right to confiscate any offensive material or illegal Mihup Communications Pvt. Ltd.'s information.

7.3 Exclusive Ownership of Developed Material

- Mihup Communications Pvt. Ltd. has exclusive rights to patents, copyrights, inventions or any other intellectual property developed by its employees.

- All programs and documents produced or provided by employees for the benefit of Mihup Communications Pvt. Ltd. are the property of Mihup Communications Pvt. Ltd. and the latter reserves the right to access and use this Mihup Communications Pvt. Ltd.'s information as it deems fit.

7.4 Restricted Uses of Mobile Device

- Only Mihup Communications Pvt. Ltd. approved portable mobile devices may be used to access organization's Information Resources.
- Portable computing devices must be password protected as per Organization's Password Policy.
- As and when required, Mihup Communications Pvt. Ltd.'s confidential data can be stored on these portable computing devices using approved encryption techniques on the data. This is subjected to approval from Top Management.
- Unattended, Mihup Communications Pvt. Ltd. provided portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet.

7.5 Teleworking

- It is the policy of Mihup Communications Pvt. Ltd. to allow employees to telework when opportunities exist for improved employee performance, reduced commuting miles, or organization savings.
- Teleworking allows employees to perform their duties outside the traditional office on a full- or part-time basis. On telework days an employee might work from home, a satellite office, or even on the road.
- Teleworking is a privilege, not a universal benefit or employee right.
- The company has the right to offer telework to an employee and to terminate a teleworking arrangement at any time. Telework is a voluntary program unless specifically stated as a condition of employment.

- Employees may decline telework if the option is presented. The employee may also discontinue the arrangement at any time, unless otherwise specified in the telework agreement.
- Telework may be temporarily suspended due to the organization's operational needs.

7.6 Internet Access

- All employees of Mihup Communications Pvt. Ltd. have Internet access at their workstations. This access can be withdrawn at any time, however, at the discretion of management.
- Internet access is monitored to ensure its proper use and compliance with security policies.
- It is forbidden to represent the company on newsgroups or in other public forums unless previously authorized by management.
- It is forbidden to place company material on publicly accessible Mihup Communications Pvt. Ltd.'s information processing systems unless so authorized by the asset owner and the Information Security Division.
- Sensitive Mihup Communications Pvt. Ltd. information such as passwords and credit card numbers should not be sent via the Internet unless encrypted.

7.7 Electronic Mail

- Mihup Communications Pvt. Ltd. provides all employees with an email address and email services in order to facilitate the performance of their tasks.
- All business communications are sent and received using this email address.
- Personal email accounts cannot be used for company business.
- Sending unsolicited emails to clients is prohibited.
- All personnel use a standard signature, which includes first and last names, business address and business phone number.
- Important messages should not be stored in the email Inbox.

7.8 Data Backup and Restoration

- Information on individual systems should be regularly backed up on a compact disc or other storage media.
- For multi-user and communications systems, the ISIC member is responsible for carrying out periodic backups.
- When requested, the ISIC provides technical assistance for the installation of backup hardware or software.
- All backup copies of critical or sensitive Mihup Communications Pvt. Ltd.'s information are stored in an approved area with controlled access.
- These copies are kept solely for the purpose of restoring the system following a computer virus infection, hard drive defects or other computer problems.
- An emergency plan is developed for all applications that handle critical operational Mihup Communications Pvt. Ltd.'s information. The Mihup Communications Pvt. Ltd.'s information owner ensures that the plan is adequately developed, frequently up-dated and periodically reviewed.

7.9 Change Management

- Company computers and communications systems used for operational activities be supported by a documented change management process that ensures only authorized changes are made.
- The change management procedure is applied whenever an important change is made to operations systems, equipment, links or procedures.
- This policy applies to PCs that run operations systems and to larger multi-user systems.

7.10 System Development Standard

- The development of operational or maintenance software by internal staff adhere to the policies set by Mihup Communications Pvt. Ltd. and to system development standards, procedures and other conventions.
- These conventions include testing, training and documentation.

7.11 Management of Licenses

- Management negotiate appropriate agreements with software suppliers regarding the need for additional licences.
- The supply service will purchase all necessary software. [List of software approved by the supply service]

8. ENVIRONMENTAL AND PHYSICAL CONTROLS

8.1 Access Control to Information and Facilities

- Access to telecommunications rooms, servers and work areas containing sensitive Mihup Communications Pvt. Ltd.'s information be restricted and only granted to employees on a need-to-know basis.
- Sensitive Mihup Communications Pvt. Ltd.'s information always is protected against unauthorized disclosure.
- Hard-copy documents containing sensitive Mihup Communications Pvt. Ltd.'s information is stored in a locked file cabinet.
- Sensitive Mihup Communications Pvt. Ltd.'s information is secured in a locked facility during non-working hours.
- A *clear desk policy* is recommended to further restrict access to documents.
- Computer screens should be positioned so as to reduce the unrestricted view of their contents.

8.2 Protection against Theft

- System and network equipment be physically secured with theft-prevention devices when located in an open office.
- Local area network (LAN) servers and other multi-user systems are placed in locked rooms.
- Portable computers (when not in use) placed in locked cabinets or secured by other theft protection devices when located in an unmonitored environment.

9. TECHNICAL SECURITY CONTROLS

9.1 User Identification and Authentication

User ID and password

- Mihup Communications Pvt. Ltd. requires all employees who access Mihup Communications Pvt. Ltd.'s information systems to have a unique user ID and a private password.
- User IDs be used in order to restrict system access privileges according to the functions, responsibilities and activities of each user.
- All employees are responsible for protecting their user IDs and passwords.

Password Choice

Information system users should choose passwords that are difficult to guess and which contain no Mihup Communications Pvt. Ltd.'s information related to their work or personal life. For example, personal ID numbers (PIN, SIN, driving licence, health insurance number) telephone numbers, names of spouses, postal addresses, proper names, known places or technical terms should not be used.

Here are some tips for creating passwords:

- Combine several words together.
- Combine punctuation or numbers with a word (upper or lower-case letters)
- Transform a common word using a specific method
- Create acronyms (initials forming a word, ex: CEGEP)
- Deliberately misspell a word.

Password Similarity

Users should not repeatedly create passwords that are identical or essentially similar to previous passwords.

Password Constraints

- Passwords contain at least 8 digits, and are changed at intervals of 90 days or less.
- The password management system obliges users to combine letters and numbers and disallows the repeated use of a password within a given time span.

Password Storage

- Passwords should not be stored in a readable form in sequential files, software macros, computers without access control systems or any other place where unauthorized persons might find them.
- Passwords should at no time be written down and left in plain sight, such on computer monitors or desks, for instance.

Password Sharing

- When Mihup Communications Pvt. Ltd.'s information needs to be shared, employees do so using emails, databases, public directories situated on local area network servers, diskettes, and other exchange media.
- Passwords should never be shared or disclosed.
- System administrators and technical staff should never ask employees to reveal their personal passwords. The only exception is in the case of a temporary password that will be changed when the user accesses the system for the first time.
- If users suspect someone is using their user IDs and passwords, it is their responsibility to immediately advise system administrators.

9.2 Malicious Software

Virus Detection Software

- System users should not cancel the process of automatic virus definition updates.
- All system files should be scanned by virus detection software.
- A scan is run before opening new data files and before executing new software.

Elimination of Viruses

- At the first sight of a possible computer virus, employees immediately cease using the affected system and call technical support.
- All magnetic storage media used on the infected computer should not be used on any other computer until the virus has been successfully removed.
- The infected computer be quarantined (isolated from the internal network).
- Users should not attempt to delete the viruses themselves.
- Qualified staff members or consultants will remove the viruses and ensure minimal data damage or destruction, and minimal downtime.

9.3 Network Security

Internal Network Connection

- All computers that store sensitive Mihup Communications Pvt. Ltd.'s information and are permanently or intermittently connected to the organization's internal computer networks have an access control system approved by the Information Security Division.
- All other types of Mihup Communications Pvt. Ltd.'s information processing systems are equipped with a screensaver password that locks after a given period of inactivity. The screen is re-activated when the correct password is re-entered.
- Multi-user systems use a session closing mechanism that automatically shuts down the user session after a given period of inactivity.

External Network Connection

- All external connections to the Mihup Communications Pvt. Ltd.'s information systems be protected with an approved dynamic password access control system. Dynamic passwords change with each use, rendering their theft useless.
- Employees should not establish connections to external networks (Internet service providers) using the organization's systems without the prior approval of the Information Security Division.

Network Changes

- Except in emergencies, all changes to the computer networks of Mihup Communications Pvt. Ltd. be recorded in a maintenance request and be approved by the Information Technologies Division.
- All changes to internal networks are carried out by personnel authorized by the Information Technologies Division.
- This process reduces the risk of unauthorized disclosure and of changes being made inadvertently during a moment of distraction without the knowledge of the Information Technologies Division.

- This process applies not only to the employees of Mihup Communications Pvt. Ltd., but also to service providers.

10. COMPLIANCE

Mihup Communications Pvt. Ltd. periodically carries out internal audits to ensure compliance with applicable policies, procedures and legislation.

10.1 Compliance with Policies and Procedures

All employees comply with Mihup Communications Pvt. Ltd.'s information security policies and related documents. Employees who, by negligence or design, violate security policies will be subject to disciplinary action.

10.2 Compliance with Legislation and Regulations

All Mihup Communications Pvt. Ltd.'s information security policies comply with applicable legislation, such as laws regarding data protection, access to Mihup Communications Pvt. Ltd.'s information, protection of personal Mihup Communications Pvt. Ltd.'s information and electronic documents, etc.

11. DISCIPLINARY MEASURES

- Suspected violations of the security policy (system hacking, virus infections) that could compromise the integrity of Mihup Communications Pvt. Ltd. information systems be immediately reported to the CISO or to the ISIC member.
- Proven violation or failure to comply with the Mihup Communications Pvt. Ltd.'s information security policy entails serious repercussions for offenders. Disciplinary measures vary in accordance to the severity of the violation.

12. REFERENCES

In order to adequately promote and support Mihup Communications Pvt. Ltd.'s information security, Mihup Communications Pvt. Ltd. has developed policies, procedures, recommendations and standards. These measures, as well as applicable legislation, are presented in the following list:

Policy

- Access control

Procedures

- Security incident management
- System formatting and reinstallation after a security incident
- Operational changes
- Personnel selection

Recommendation

- ISO 27001 Standard

Legislation

- IT Act 2000
- Copyright Act