Document Code	MHRL-IT-PO01/1.0
Effective Date	April 05, 2024
Name	Information Technology Policy Framework
Version	1.0
Classification	Internal
Owner of this Policy	Head of IT

Purpose

This is the Information Technology Security System (ITSS) of MHRL. The purpose of this policy is, to secure the group's Information Technology assets and the data created, stored, processed, and deleted from it. However, it by and large focuses on securing this asset solely from a technological angle. Physical risks and social risks are out of the scope of this document. Addressing these issues here would develop the ITSS towards a full-fledged Information Security Management System (ISMS), which is recommended to be done at a later stage.

Scope

This IT Policy applies to

- All computers connected to MHRL admin network in any of the business units; and
- All MHRL employees, trainees, temporary staff, third party personnel and any other person who have been granted the right to use the company's IT resources or services.

The documentation of the framework in its current version consists of 33 documents, including 17 Policies and 16 Forms.

Policy

The documentation is structured across four functional areas: Policies, Procedures and Forms.

A **Policy** is a document outlining certain norms which the organization wants to enforce.

A **Form** is a document that has to be filled while following a process, to control process adherence and assure process conformance.

The Policies have been grouped as follows:

- Users Related Policies
- IT Administration Policies
- Backup & Recovery Policies
- Partner, Vendor & Other Third Party related policies
- Information & Cyber Security Policies
- Policies related to Document Control for ITSS

Policy

Users Related Policies

- **Information Technology Acceptable Use Policy (MHRL-IT-PO02)** These are provided to every employee and Third party representatives on engaging with MHRL. These cover General Security Policy, Acceptable Use of internet & email and Password Standards. The users must sign the **Acceptable Use Agreement (MHRL-IT-FO11)** as acknowledgement.
- **Laptop, Mobile Computing and Communication Policy (MHRL-IT-PO11)** guiding IT Administrator how to secure all mobile platforms technically. This policy guides users how to use mobile platforms securely when out of office.
- **Password Management Policy (MHRL-IT-PO15)** establishes the standards for strong passwords andthe frequency of change and also prescribes the standards for password protection and sharing.
- **Internet Policy (MHRL-IT-PO16)** provides guidelines for Internet access for official purpose and defines the types of sites allowed / disallowed.
- **Acceptable Use Agreement Form (MHRL-IT-FO11)** to be signed by everyone as acceptance of theAcceptable Use Agreement.
- **User ID Requisition Form (MHRL-IT-FO12)** to standardize the process of creation , maintenance and deletion authorization for user ID management betweenFunctional Heads and the IT department.
- **Asset Allocation Form (MHRL-IT-FO13)** to create standard documentation and keep track of digital assets belonging to the company..
- **Personal Equipment Authorization Form (MHRL-IT-FO17)** to approve and record authorization for use ofpersonal equipment to connect with MHRL Group network.

IT Administration Policies

- **Data Handling, Retention, Storage & Disposal of Media Policy (MHRL-IT-PO03)** Specifies roles, responsibilities and reporting for users and administrators on handling data and information of various types in the company.
- **Antivirus & Patch Management Policy (MHRL-IT-PO04)** Prescribes planning, purchasing and automating antivirus as well as software components of companies IT system.
- **IT Administrator Policy (MHRL-IT-PO07)** Guideline for administrators to protect MHRL's resources fromunauthorized access while facilitating seamless and legitimate use of these resources.
- **Equipment Configuration Policy (MHRL-IT-PO08)** process of configuration to secure all externally facing devices, like firewalls & routers.

Policy

- **Remote Access Policy (MHRL-IT-PO10)** to The process and routine to keep MHRL's network safe when out-of-office staff or third parties have to remotely access the network.
- **IT Standards Policy (MHRL-IT-PO13)** establishes the standards for all IT Assets in use in MHRL.
- **Wireless LAN Policy (MHRL-IT-PO14)** prevents the wireless LAN from vulnerabilities and to promote use of industry standards in the network establishment, maintenance and upgradation.
- **IT Standard Tasks and Documents (MHRL-IT-PO17)** to prescribe in detail different routines of the IT teams at Corporate and at different locations.
- **Monitoring Request Form (MHRL-IT-FO14)** Prescribed format for authorization to IT to facilitate monitoring off different IT foot prints of an employee
- **Laptop, Data card & Storage Device Exception Form (MHRL-IT-FO15)** enables to request exceptions to the rule prohibiting transportation of information on USB storage devices.
- **Wireless LAN & Bluetooth Network Exception Request (MHRL-IT-FO16)** to ask for the permission to establish a business critical wireless network at MHRL's premises.
- **Mailbox Size Exception Request (MHRL-IT-FO19)** to apply for larger size of mailbox.
- **List of AMC (MHRL-IT-FO22)** to have a consolidated list of all IT related maintenance contracts along with the key terms & details.
- **Software License Inventory & Compliance Form (MHRL-IT-FO23)** for consolidated view of the software licenses and compliance thereof at different units and corporate office.
- **IT Assets Inventory List (MHRL-IT-FO24)** for consolidated view of all IT assets existing in different units and corporate office.

Policy

Backup & Recovery Policies

- **Backup & Recovery Policy (MHRL-IT-PO05)** prescribes different methods and processes for regular backup and testing of the backups for recovery and business continuity purposes across the company.

- **Backup Plan & Schedule (MHRL-IT-PO06)** defines Application Owner-wise, Backup frequency, Backup mechanism, Retention Plan, Offsite frequency, Offsite Location, etc. It is meant to be used MHRL ether with the Backup & Recovery Policy.

- **Backup Record (MHRL-IT-FO08)** to organize, document, track, and trace backups taken at all locations.

- **Recovery Drill Reporting Form (MHRL-IT-FO09)** to help the IT teams and the Head Corporate IT to check if backups taken are successful and bring in enhancements wherever required.

Partner, Vendor & Other Third Party related policies

- **Information Technology Acceptable Use Policy (MHRL-IT-PO02)** must be by every Third party representative along with company employee concerned wherever necessary, on engaging with MHRL. It covers General Security Policy, Acceptable Use of internet & email and Password Standards. The signatory must sign the **Acceptable Use Agreement (MHRL-IT-FO11)** as acknowledgement

- **Non-disclosure Agreement (MHRL-IT-FO05) an agreement for partner, vendor and other third parties prescribing the manner and method of** confidential and sensitive information.

Information & Cyber Security Policies

- **Information Classification Policy (MHRL-IT-PO09)** to ensure that all documents are rated according to their confidentiality.

- **Asset Criticality Policy (MHRL-IT-PO12)** governs the criticality ratings of assets.

Point of Contact

Manager IT Infrastructure, Unit IT In-charge

Responsibility

Corporate: Manager IT Infrastructure, GM-IT

Unit: Unit IT In-Charge, Finance Head

Exception and Exception Handling

This Policy needs to be revised with every document being included or removed from the documentary body. Moreover, the document should be reviewed every year after its last revision.