MOREPEN LABORATORIES LIMITED

CIN: L24231HP1984PLC006028

Registered Office: Village Morepen, Nalagarh Road, Near Baddi Distt. Solan, Himachal Pradesh–173 205
Email: plants@morepen.com, Website: www.morepen.com,
Tel.: +91-1795-266401-03, 244590, Fax: +91-1795-244591

Corporate Office: 2nd Floor, Tower C, DLF Cyber Park, Udyog Vihar-III, Sector-20, Gurugram, Haryana-1221016; Email: corporate@morepen.com, Website: www.morepen.com,
Tel.: +91-124-4892000

ACCEPTABLE USAGE POLICY

Table of Contents

1. Purpose

1.1 Acceptable Usage Policy has been laid to avoid exposure of Morepen Laboratories Limited information assets to any risk arising from events like virus attacks, compromise of network systems and services, and legal issues, which might arise due to inappropriate and improper usage, whether accidental or deliberate.

1.2 The objective of this policy is to set the scope of employee responsibilities in order to strengthen and maintain the information security of Morepen Laboratories Limited

2. Scope

This policy applies to all employees, consultants, vendor staff, trainees, and other personnel working for Morepen Laboratories Limited physically or virtually from any location approved by Morepen Laboratories Limited.

3. Rules

3.1 All the users are briefed about the acceptable usage of the information resources before being granted access.

3.2 Any unacceptable usage identified results in initiation/warning of disciplinary action against the concerned user.

3.3 For security and network maintenance purposes, authorized individuals within Morepen Laboratories Limited may monitor equipment, systems and network traffic at any time.

3.4 Management reserves the right to review information assets assigned to users to ensure compliance with this policy.

4. Procedure

4.1 General Usage During Employment

4.1.1 Users shall use Morepen Laboratories Limited's authorized cloud storage service or servers to store only their official files/data.

4.1.2 Users shall be restricted from installing any software/application tools on their own. The requester's manager approval shall be required and reviewed by the IT team before installation of any additional software/application.

4.1.3 The employee shall not use Morepen Laboratories Limited facilities for personal profit-making or commercial activity.

4.2 Bring Your Own Device Policy (BYOD)

4.2.1 BYOD practice shall be discouraged and shall only be approved for business needs.

4.2.2 BYOD laptops must not have any privileged tools or scanning software installed and must have basic security tools/parameters/configurations equivalent to standards set by Morepen Laboratories Limited.

4.2.3 Approved devices must comply with Morepen Laboratories Limited Information Security policy.

4.2.4 Smartphones and iPads are not permitted privileged access to the production environment and must keep their devices updated with the latest security patches.

4.2.5 Smartphones and tablets may access the internet and corporate email server (IMAP).

4.2.6 Employees should avoid saving personal confidential data on laptops used for company purposes.

4.2.7 Morepen Laboratories Limited can access, copy, delete, or remotely wipe data on personal devices approved for network access. MLL owns all data and software on such devices.

4.2.8 Users shall not download/install any file or software from the Internet on Morepen Laboratories Limited provided assets.

4.3 Complying with Copyright Licensing and Protecting Intellectual Property

4.3.1 All software used on organization information processing facilities shall be procured in accordance with official organization policies and procedures defined based on the business requirement and shall be licensed & registered in the name of the Corporation.

4.3.2 All personnel shall abide by software copyright laws and shall not obtain, install, replicate, or use software by unethical means.

4.3.3 To ensure the integrity of organization-developed software, all personnel shall abide by the intellectual property protection contract provisions of the corporation.

4.4 Clear Desk and Clear Screen

4.4.1 At the end of each workday, employees must ensure that their desks are free from confidential or sensitive information.

4.4.2 All sensitive documents and materials must be stored securely in locked drawers or cabinets when not in use. Access to these storage areas should be restricted to authorized personnel only or when leaving their desks for an extended period.

4.4.3 Any confidential or sensitive documents that are no longer needed must be disposed of securely using shredders or designated confidential waste bins.

4.4.4 Employees must lock their computer screens when leaving their workstations unattended, even for short periods.

4.4.5 Computers should be configured to automatically lock after a period of inactivity, preferably no more than 15 minutes.

4.4.6 Employees must log out of all systems and applications containing sensitive information at the end of the workday or when the device will not be used for an extended period.

4.4.7 Ensure sensitive information on screens is not visible to unauthorized individuals and use privacy screens and never leave devices unattended in public places.

4.5 Internet over Wi-Fi

Access to the Internet is available to all employees, contractors, subcontractors, and business partners, whose duties require it for the conduct of the organization's business. Since Internet activities may be monitored.

4.5.1 Acceptable Use

The corporation provides Internet access to facilitate the conduct of the organization's business. Occasional and incidental personal Internet use shall be permitted if it does not interfere with the work of personnel, the corporation's ability to perform its mission, and meets the conditions outlined in official organization directives.

4.5.2 Prohibited Use

4.5.2.1 Browsing explicit pornographic or hate-based websites, hacker or cracker sites, or other sites that the corporation has determined to be off-limits.

4.5.2.2 Posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, hacker-related material, or other material determined to be off-limits by the organization.

4.5.2.3 Posting or sending sensitive information outside of the corporation without the information owner's authorization.

4.5.2.4 Posting commercial announcements or advertising material.

4.5.2.5 Promoting or maintaining a personal or private business.

4.5.2.6 Using non-work-related applications or software that occupy excess workstation or network processing time (e.g., processing in conjunction with screen savers).

4.6 E-mail Usage

4.6.1 Morepen Laboratories Limited shall use a secure solution to provide the email facility to its employees.

4.6.2 Morepen Laboratories Limited's email solution shall have adequate controls to take care of security risks such as identity management, viruses, etc.

4.6.3 Using a reasonable amount of Morepen Laboratories Limited resources for personal emails is unacceptable.

4.6.4 Sending chain letters, and threatening or offensive emails from the Morepen Laboratories Limited email account is prohibited

4.7 Virtual Private Network (VPN)

4.7.1 VPN connections are allowed only to Morepen Laboratories Limited employees to securely access a corporate intranet while located outside the office & all will securely connect with applied policies.

4.7.2 It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed to access the organization's internal network.

4.7.3 All computers connected to the organization's internal network via VPN, or any other technology must use the most up-to-date antivirus software that is the corporate standard, this includes personal computers.

4.7.4 When using VPN technology with personal equipment, users must understand that the machine is exposed to the extension of the organization's network and, as such, is subject to the same rules and regulations that apply to organization-owned equipment, i.e., their machines must be configured to comply with the organization's Security Policy.

4.7.5 VPN to be used only after approval of ISMS/designated officer.

4.8 Mobile Computing Devices

4.8.1 The employee shall take appropriate care while using mobile computing devices which may have confidential MLL's data.

4.8.2 The employee shall never leave their PDAs, Cellular Phones, Digital diaries, USB Drives etc. unattended.

4.8.3 The employee shall use a power-on password for their mobile computing devices.

4.8.4 Morepen Laboratories Limited shall ensure that the use of mobile devices does not lead to a compromise of Personal Identifiable Information.

4.9 E-Security

4.9.1 Change temporary passwords at the first log-on.

4.9.2 Select quality passwords with a minimum of 8 characters

4.9.3 All hosts used by the employee that are connected to the organization's Internet/Intranet/Extranet, whether owned by the employee or the organization, shall be continually executing approved virus-scanning software with a current virus pattern/signature. In case Antivirus software is missing from the user's PC and Server then IT should be informed immediately.

4.9.4 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty is prohibited.

4.9.5 Installation of any wireless equipment on the company premises or its proximity is not allowed without prior permission.

4.9.6 Personal chatting on the internet is disallowed. In special cases, where chatting with external clients is required, authorization is given by the project manager which is approved by the Head of Software Development.

4.10 Blogging/ Social Media

4.10.1 Employees must follow company policies when using the Internet, including blogging and social networking. Discussing business or proprietary information in public forums is prohibited to avoid workplace disruptions and protect the company's reputation.

4.10.2 Do not disclose confidential or proprietary information, trade secrets, or company-related material on blogs or social networks. Personal statements should not be attributed to the company. Disrespectful communications linked to the company are prohibited.

4.10.3 Blogs reflect personal views, not the company's. Employees mentioning the company or their employment on social media must include a disclaimer: "The views expressed here are my own and not those of my employer."

4.11 USB blocking

To protect Information and Communication Technology (ICT) infrastructure from cyber security threats, MLL shall implement an endpoint security solution to block all USB devices in machines/desktops and will allow only authorized sanitized devices in Morepen Laboratories Limited.

5. Enforcement

All employees are expected to comply with the Acceptable Usage Policy. Non-compliance with the same may result in disciplinary action or punishment, which shall vary as per the severity of the incident.