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

ACCESS CONTROL POLICY

Sandeep atri
Signed by Sandeep Atri, Title: IT Head, Org: Morepen Laboratories Ltd..

TABLE OF CONTENTS

1. Policy

1.1 This policy outlines the access controls implemented on information assets associated with Morepen Laboratories Limited.

2. Purpose

2.1. The purpose of the policy is to implement Access Control across all IT systems and services in order to provide authorized and appropriate user access and to ensure appropriate preservation of data Confidentiality, Integrity and Availability.

3. Scope

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

4. Rules and Procedures

4.1. Access Control Principles

4.1.1. Morepen Laboratories shall provide all employees and other users with the information they need to carry out their responsibilities in an effective and efficient manner on a “need to know basis”.

4.1.2. Generic IDs shall not be permitted, but may be granted, with authorization under exceptional circumstances, if there is an explicit business requirement, wherein the confidentiality of secret authentication information shall be maintained when shared.

4.1.3. Access rights will be accorded following the principle of least privilege, security, asset classification and need to know. Access to information and application system functions shall be restricted.

4.1.4. Access to systems and applications should be controlled by a secure log-on procedure.

4.1.5. Every user must attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.

4.1.6. Users are obligated to report instances of non-compliance (such as unauthorized access, compromised critical systems, data theft, data corruption, data deletion, ransomware attacks, disruption to business activities, misuse of privileged access) to their immediate manager/senior.

4.1.7. Instances of non-compliance may be treated through the incident management process.

4.1.8 Personnel with elevated system access entitlements shall be closely supervised with all their systems activities logged and periodically reviewed.

4.1.9 Morepen Laboratories shall adopt multi-factor authentication for users of having access to:

4.1.9.1 Morepen Laboratories Critical information systems.

4.1.9.2 For critical paper information (Valid ID/Access card + Valid Approval)

4.2. User Access Management

4.2.1. User Registration and deregistration

4.2.1.1. No access to any Morepen Laboratories IT resources or services will be provided / activated to the users, without authentication and authorization process being completed. The authorization shall be approved by the Asset owner or delegated authority.

4.2.1.2. Every user should be provided with a unique user ID and Password.

4.2.1.3. The level of access granted for each of the privileged access rights associated with a system or process shall be appropriate to the access control principles and be consistent with other requirements such as segregation of duties.

4.2.1.4. The Morepen Laboratories User ID to be created as per the below convention, primarily for Email IDs but is suggested to be followed for all new user creation in other applications.

4.2.1.5. First name of an employees or contractual employee.
In case of clash of first name, first name and Last name is to be used. Further, in case of clash of first name and last name for any employee numeric digit to be suffixed with last name, e.g., Navin.Chandra and navin.chandra1 for two user with the same first and last name.

4.2.1.6. When an employee or contractor is terminated/leaves, all of their IDs and passwords or other means of accessing files or using computer resources shall be disabled or removed within 24 working hours of their departure. For re-allocation, employee ID and access to e-mail and other administrative access shall be retained.

4.2.1.7. It is the responsibility of the Asset owner to deactivate / re-allocate or delete any of the provisioned access of the terminated / transferred employee, as per the requirement of the business process. The Asset owner or delegated authority shall inform the HR, using the no-dues form, of clearance related to Access de-registration.

4.2.1.8. When access control of users, who administer or operate systems and services that process PII, is compromised or likelihood of it being compromised, the user must report the incident directly to the IT team and shall subsequently report the same through the Incident reporting procedure. It is the responsibility of the user whose access control may have been compromised, to escalate the issue, if required, when corporative action is not implemented, within 1 hour of reporting the compromise.

4.2.1.9. Morepen Laboratories shall not reissue to users any deactivated or expired user IDs for systems and services that process PII.

4.2.1.10. The allocation of privilege rights (e.g. server administrator, super-user, root access) shall be restricted and controlled and authorization provided as per the roles and responsibilities mentioned in Information security organization structure document.

4.2.1.11. Privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged ID.

4.2.1.12. The competences of users with privileged access rights should be reviewed annually in order to verify if they are in line with their duties.

4.2.1.13. Access to Confidential information and privileged access shall be limited to authorized persons whose job responsibilities require it, as determined by the respective Department Heads. Requests for privilege access permission to be granted, changed or revoked must be made through the approval process and logged.

4.2.1.14. Access for remote users shall be subject to only through VPN. Multi-factor authentication should be implemented in VPN. No uncontrolled external access shall be permitted to any production system.

4.2.1.15. The Morepen Laboratories records shall specify the expiry of the privilege access rights.

4.2.1.16. For each third party/ vendor, a separate user id shall be created for each user. Access to IT systems can be given via remote access solutions (Exp.- Anydesk) based on the business requirement.

Sandeep atri Signed by Sandeep Atri, Title: IT Head, Org: Morepen Laboratories Ltd..

4.2.2. Access Control Methods

4.2.2.1. Access to data and user authentication is variously and appropriately controlled according to the business requirement of the user which shall be approved by the respective department heads.

4.2.2.2. Access control and authentication methods may include logon access rights, 2 Factor authentication, user account privileges, server and workstation access rights, firewall permissions, Database rights, isolated networks and other methods as deemed necessary.

4.2.3Role based Access Control

4.2.3.1 Access to information should be based on well-defined user roles (system administrator, user manager, application owner etc.), Morepen Laboratories shall avoid dependency on one or few persons for a particular job. There should be clear delegation of authority for the right to upgrade/change user profiles and permissions and also key business parameters which should be documented.

4.2.4Access Control Review

4.2.4.1 Access review for production environment shall be conducted every 6 months by the IT HOD.

4.2.4.2 Access review for code repository shall be conducted every 6 months by the IT HOD.

4.2.4.3 Access review for critical and high rated applications shall be conducted every 6 months and for medium every 1 year and low rated applications every 2 years by the IT HOD.

4.3 System and Application Access control

4.3.1Information Access Restriction.

4.3.1.1 Restrictions to access shall be based on individual business application requirements. The following shall be considered in order to support access restriction requirements, as applicable:

Sandeep atri
Signed by Sandeep Atri, Title: IT Head, Org: Morepen Laboratories Ltd..

4.3.1.2 Controls to manage access to application system functions and data.

4.3.1.3 Controls to limit the information contained in outputs.

4.3.1.4 Implementation for physical or logical access controls for the isolation of sensitive applications, application data, or systems.

4.3.2Secure Log-on Procedures

4.3.2.1 Morepen Laboratories shall adopt login procedures that minimize the opportunity for unauthorized access by implementing security controls.

4.3.2.2 The operating systems of servers, workstations, and/ or network devices shall be designed to minimize the opportunity for unauthorized access.

4.3.2.3 The log-on controls shall:

4.3.2.3.1 Validate the log-on information on completion of login input data. If an error condition arises, the system shall not throw the error message leaking out internal configurations of the system/applications/databases.

4.3.2.3.2 Discourage help messages during the log-on procedure that would aid an unauthorized user.

4.3.2.4 Ensure terminal lockout after 15 minutes of inactivity. Exception to this should be approved, logged and monitored.

4.3.2.5 Display a general warning notice/ banner that the computer should only be accessed by authorized users.

4.3.3 Password Management

4.3.3.1 Users shall change passwords whenever there is any indication of possible system or password compromise.

4.3.3.2 Select strong passwords based on the following:

4.3.3.2.1 Should be at least eight alphanumeric characters long.

4.3.3.2.2 Contain both upper and lower case characters (e.g., a-z, A-Z)

4.3.3.2.3 Have digits and punctuation characters as well as letters, e.g.,0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

4.3.3.2.4 Passwords should never be written down or stored on-line.

4.3.3.2.5 All email passwords shall be changed after 90 days. Production passwords (including servers) shall be changed after 90 days. Root / Admin passwords to be stored in a secure vault, with access by IT HOD only.

4.3.3.2.6 Vendor-supplied passwords for applications and devices shall be changed after installation. The password shall be modified based on the above guidelines as applicable.

4.3.3.3 When users are required to maintain their own secret authentication information, they should be provided initially with secure temporary secret authentication information, which they are forced to change on first use.

4.3.3.3.1 Temporary secret authentication information should be given to users in a secure manner. The user ID and Secret information shall be sent by different communication modes and if sent collectively over mail, the mail content shall be encrypted. The key shall be sent through a different communication mode.

4.3.3.3.2 Users should acknowledge receipt of secret authentication information.

4.3.3.4 The Head of the department, approving the Access creation of a user, shall ensure the identity of a user prior to providing new, replacement or temporary secret authentication information. The mode for sharing the first login credentials shall be shared by the head of HR, during induction and at other times by the Head of the department of the user.

4.3.3.5 Root passwords/ Admin passwords to the servers to be available only with select members of the team on “need to know” basis.

4.3.3.6 General password management guidelines:

4.3.3.6.1 Do not reveal a password to anyone including seniors.

4.3.3.6.2 Do not disclose a password in front of others.

4.3.3.6.3 Do not hint at the format of a password (e.g., "My family name")

4.3.3.6.4 Do not reveal a password on questionnaires or security forms.

4.3.3.6.5 Do not share a password with family members.

4.3.3.7 Do not enable the "Remember Password" feature of applications.

4.3.3.8 Do not write passwords down and store them anywhere in the office. The exception to the same may be for storing some privileged user passwords in a secure vault for Business Continuity purposes.

4.3.3.9 Do not store passwords in a file on any computer system without encryption.

4.3.3.10 If an account or password is suspected to have been compromised, report the incident to Management and change all passwords.

4.3.3.11 Passwords used as secret authentication information in automated log-on procedures shall remain encrypted at rest.

4.3.4 Use of Privileged System Utility Program

4.3.4.1 The privileged system utility Program shall have tightly control access and limited permissions, and associated monitoring when these programs are allowed to run.

4.3.4.2 The System Utilities shall be controlled using identification, authentication and authorization procedures.

4.3.4.3 Executable code shall be implemented in the production environment in compliance with the SDLC Procedure.

4.3.4.4 The use of utility programs, development, production, and test environment shall all be independent and segregated.

4.3.4.5 The use of utility programs shall be reviewed on an annual basis and unnecessary programs shall be disabled or deleted.

4.3.4.6 The version control of all programs shall be maintained.

4.3.5Access Control to Confidential information

4.3.5.1 Valuable or sensitive information or data including Proprietary, Intellectual property, source code, research data, and Customer data, the release of this information or data may affect organization or adversely reflect on the company or its employees. Access to this data is only permitted to workforce members who have valid business needs.

4.3.5.2 Access control to program source code is as specified in software development lifecycle procedure.

5 Logical Access Management Procedures

5.1 General Principles

5.1.1 Morepen Laboratories will have a process of appropriate checks and balances in regard to personnel with privileged access like IT administrator, cyber security personnel, authorized application owners/users. The said employees should be subject to background check and screening.

5.1.2 Morepen Laboratories shall avoid dependence on one or few persons for a particular job. The access to information should be based on well-defined user roles (system administrator, application owner, database admin, etc.). Application level 'Roles' and corresponding access rights in applications will be well-defined based on related job functions.

5.1.2.1 The following Roles and related access rights will be segregated:

5.1.2.1.1 Rights to upgrade/change user profiles and permissions (based on relevant approvals from authorized business heads) will be with the IT Head, based on approved permission(s).

5.1.2.1.2 Authority to approve a change key business parameter /system master will be with the Application owners although the configuration will be done/ changed by the IT Administrator.

5.1.2.1.3 Maker-checker shall be implemented for transaction processing. For each transaction, there must be at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information.

5.1.2.1.4 IT Head shall ensure that there should be a clear segregation of responsibilities relating to system administration, database administration and transaction processing.

6 Enforcement

6.1 All employees are expected to comply with the Access Control Policy. Non-compliance may result in disciplinary action or punishment, which shall vary as per the severity of the incidence.

Sandeep atri

Signed by Sandeep Atri, Title: IT Head, Org: Morepen Laboratories Ltd..