ACCESS CONTROL POLICY

1. Purpose

The purpose of this policy is to ensure the secure access and usage of Enterprise Resource Planning (ERP) systems and G Suite applications within Quality Asia. This policy outlines the procedures and guidelines for granting, managing, and revoking access to ERP and G Suite resources to maintain data confidentiality, integrity, and availability.

2. Scope

This policy applies to all employees, auditors, contractors, third-party vendors, and any other individuals granted access to ERP and G Suite systems on behalf of Quality Asia.

3. Roles and Responsibilities

System Administrator: Responsible for configuring access controls, managing user accounts, and overseeing system security settings within ERP and G Suite.

User: Responsible for adhering to access control policies, safeguarding login credentials, and using ERP and G Suite resources in accordance with organisational guidelines.

4. Access Control Principles

Role-Based Access Control (RBAC): Access to ERP and G Suite resources will be based on predefined user roles and permissions assigned according to job responsibilities and organisational needs.

Principle of Least Privilege: Users will be granted the minimum level of access necessary to perform their assigned tasks within ERP and G Suite applications.

Authentication and Authorization: Users must authenticate themselves using approved methods (e.g., username/password, multi-factor authentication) before accessing ERP and G Suite resources. Access will be authorised based on the user's role and permissions.

Data Classification: Data within ERP and G Suite will be classified based on sensitivity levels, and access controls will be applied accordingly to ensure appropriate protection of data.

Audit Trails and Monitoring: Access to ERP and G Suite resources will be logged, monitored, and reviewed regularly to detect and prevent unauthorised access or misuse.

5. Access Control Procedures

User Account Provisioning: User accounts will be provisioned based on Management System Records and Requirements. System administrators will create user accounts and assign appropriate roles and permissions

User Account Deactivation: User accounts will be deactivated promptly upon termination of employment, contract expiration, or change in role. Access to ERP and G Suite resources will be revoked to prevent unauthorised access.

Access Requests and Approvals: Requests for additional access or modifications to existing access privileges must be submitted through the Document Change Request in ERP.

Periodic Access Reviews: Access permissions will be reviewed periodically to ensure alignment with current job responsibilities and organisational needs. Any discrepancies or unauthorised access will be addressed promptly.

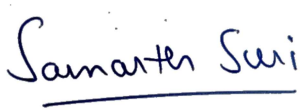
6. Training and Awareness

All users granted access to ERP and G Suite resources will receive training on Access Control Policy, Information Security Policy, and Information Security Best Practices. Regular awareness sessions will be conducted to reinforce the importance of safeguarding sensitive information and adhering to access control guidelines.

7. Compliance

This policy complies with relevant laws, regulations, and industry standards governing data privacy and security.

Quality Asia Certifications Private Limited



Managing Director

Date - 01-04-2023