1. Objective

The purpose of access control is to ensure that only authorized individuals, devices, software components, and services can access the Organization's information and other associated assets, and that unauthorized access is prevented. Access control is implemented to protect the confidentiality, integrity, and availability of information by establishing consistent rules for who may access which assets, under what conditions, and with what level of privilege.

The objectives of this Policy are to: (i) define access control principles and the Organization's access control approach; (ii) ensure access is granted based on business need and risk, and is formally authorized; (iii) reduce the likelihood and impact of unauthorized access, misuse of privileges, fraud, and error; (iv) ensure access rights remain appropriate over time through periodic review and timely revocation; and (v) maintain accountability and traceability for access to sensitive information and critical systems.

2. Scope

This Policy applies to the entire Organization and all persons who access the Organization's information and other associated assets, including employees, contractors, temporary staff, consultants, interns, and third parties (including suppliers, service providers, and partners). It applies to all environments where the Organization's information is processed, stored, or transmitted, including on-premises systems, endpoints, applications, databases, networks, facilities, cloud services, mobile devices, and remotely accessed resources.

This Policy covers access to all information assets regardless of format, including electronic information, paper records, verbal information, and physical media. It applies to all systems and services used to manage identity, authentication, authorization, monitoring, and audit logging.

3. Policy Statement

Access to information and other associated assets shall be controlled through defined and implemented rules that reflect business requirements, information security requirements, risk, and applicable legal and contractual obligations. Access rights shall be granted only when there is a legitimate business requirement, shall be limited to what is necessary to perform assigned duties, and shall be managed throughout the identity and access lifecycle, including provisioning, modification, periodic review, and removal.

4. Access Control Principles

The Organization implements access control according to the following mandatory principles.

Need-to-know is required for all non-public information. Access shall be granted only to individuals and entities with a justified business need for the specific information and only for the period that need exists.

Least privilege is required for all access, including administrative and service access. Users and entities shall be granted the minimum set of access rights necessary to perform authorized tasks, and elevated privileges shall not be granted by default.

Default-deny is enforced. Access to systems, applications, networks, and information is prohibited unless explicitly authorized. Where feasible, systems shall be configured so that access is denied by default and only permitted through approved access rules.

Anonymous access to sensitive or classified information is prohibited. Access to sensitive information shall not be permitted by unknown identities or anonymously. Where public access is required for business purposes, it shall be limited to storage locations and services that do not contain sensitive information and are explicitly designated for public use.

Accountability and traceability are required. Access to systems and information shall be attributable to a unique and controlled identity, except where a documented and approved exception is granted for shared identities that are operationally necessary and can be managed with compensating controls.

Segregation of duties is required. Access rights shall be designed and administered to reduce the risk of fraud, error, or circumvention of controls. Incompatible duties (such as requesting access, approving access, and implementing access) shall be separated where practicable.

5. Access Control Model

The Organization uses **Role-Based Access Control (RBAC)** as the primary access control model. Roles are defined based on business functions and job responsibilities and are approved by Management and relevant asset owners. Role definitions specify permitted access to systems and data, including rights such as read, write, modify, delete, and execute, as applicable.

Permissions are assigned to roles and then granted to individuals through role assignment rather than direct entitlement where feasible. Exceptions that require user-specific entitlements

shall be minimized and must follow the same authorization and review requirements as role-based access.

Where RBAC alone is insufficient due to technical or business needs, the Organization may implement additional mechanisms such as **Access Control Lists (ACLs)** or attribute-based access controls (for example, using attributes such as system sensitivity, location, device posture, time, or network context). Such mechanisms shall remain consistent with the principles in this Policy, particularly least privilege, default-deny, and need-to-know.

6. Identity Management and Authentication

All access to the Organization's systems and information shall be associated with managed identities. Identity creation, modification, suspension, and deletion shall follow a controlled lifecycle process integrated with joiner–mover–leaver events and contractual onboarding/offboarding for third parties.

Where identities are assigned to persons, each identity shall be uniquely linked to a single individual to support accountability. Shared identities shall be avoided and permitted only when operationally necessary, explicitly approved, and managed with documented compensating controls such as restricted scope, enhanced monitoring, and periodic reconciliation of use.

Authentication methods and strength shall be commensurate with the access restrictions and the classification of information being accessed. The Organization shall implement secure authentication technologies and procedures appropriate to the risk, including multi-factor authentication where required by system sensitivity, privileged access, remote access, or other risk factors.

Authentication information (including passwords, cryptographic keys, tokens, certificates, and secrets) shall be allocated and managed through a controlled process. Authentication information shall be protected against unauthorized disclosure, sharing, guessing, or interception, and shall be stored and transmitted using approved secure mechanisms. Users shall not share authentication information, and the Organization shall provide clear handling requirements for all authentication mechanisms in use.

7. Access Authorization and Approval

Access shall be granted only following formal requests and approval. Access requests must specify the requester's identity, the required asset(s), the requested level of access, the business justification, and the intended duration where access is time-bound.

Authorization responsibility is assigned to the relevant asset owner or designated system owner, who shall validate the business need, ensure alignment with classification and handling requirements, and confirm compliance with segregation of duties. The function responsible for implementing access (for example, IT Operations, Security Operations, or system administrators) shall not approve its own access and shall only implement access that has been properly authorized.

Access approvals and implementations shall be recorded in an auditable manner, including the approver identity, timestamp, scope of access granted, and any conditions or expiry dates. Emergency or expedited access shall be permitted only under documented emergency procedures with retrospective approval and review.

8. Access Rights Management and Lifecycle Controls

Access rights shall be provisioned, reviewed, modified, and removed in accordance with this Policy and the Organization’s topic-specific access control rules. Access shall be adjusted promptly when a user’s role changes, when responsibilities change, or when there is a change in business need.

Upon termination of employment or contract, access shall be revoked in a timely manner consistent with risk and operational requirements. For third parties, access shall be time-bound wherever feasible and removed at contract end, upon disengagement, or when no longer required.

The Organization shall maintain records of access rights and changes to access rights sufficient to support audit, investigation, and compliance needs.

9. Privileged Access

Privileged access rights (including administrative rights and other elevated permissions that can override system controls) shall be restricted and managed. Privileged access shall be granted only to individuals who require it to perform authorized administrative tasks and who have appropriate competence and authorization.

Privileged accounts shall be subject to enhanced controls, which include stricter authorization, stronger authentication, monitoring, and periodic review. Privileged identities shall not be shared across multiple persons, and generic administrative identities shall be avoided where possible; where technically unavoidable, their use shall be tightly controlled and monitored.

Privileged access shall be used only for administrative activities and not for day-to-day general tasks. Where feasible, the Organization shall implement time-bound privileged elevation (for

example, “break-glass” access) to reduce standing privileges, with associated logging and post-use review.

10. Access Review

Access rights shall be reviewed periodically to confirm ongoing appropriateness. Reviews shall occur at a frequency determined by risk and business context and shall be more frequent for privileged access and high-impact systems. At minimum, access rights shall be reviewed at least annually, and additionally upon significant organizational change, system change, security incidents affecting access, or major role changes.

Access reviews shall validate: continued business need, role alignment, least privilege, segregation of duties, appropriateness relative to information classification, and compliance with authorization records. Any discrepancies shall be remediated promptly, including removal or reduction of excessive permissions.

11. Logical and Physical Access

Logical access controls (to systems, applications, networks, cloud services, and data repositories) shall be designed and implemented to enforce this Policy’s principles and to reflect the classification of information and associated handling requirements.

Physical access to facilities and secure areas where information and other associated assets are processed or stored shall be controlled to ensure only authorized physical access occurs. Secure areas shall be protected by appropriate entry controls and access points, and physical access rights shall be aligned with job responsibilities and business need, and shall be reviewed and revoked in line with the same lifecycle expectations applied to logical access.

12. Monitoring, Logging, and Detection

Access-related events shall be monitored proportionate to risk. Systems supporting sensitive information or privileged activity shall implement enhanced monitoring to detect unauthorized access attempts, privilege misuse, anomalous access patterns, and policy violations.

Logs that record relevant activities, exceptions, faults, and other events shall be produced, stored, protected, and analyzed to support operational assurance, investigation, and compliance. Logging and monitoring shall be implemented in accordance with applicable retention requirements, privacy obligations, and the Organization’s event management processes.

13 Exceptions Management

Exceptions to this Policy are permitted only when a legitimate business requirement cannot be met through standard controls. All exceptions shall be formally documented, including the specific requirement being excepted, scope, duration, justification, risk assessment, and compensating controls.

Exceptions require approval by the asset owner, the ISMS Manager (or delegated security authority), and relevant Management, based on the assessed risk. Exceptions shall be time-bound wherever feasible and shall be reviewed periodically to confirm continued necessity and effectiveness of compensating controls. Exceptions shall be revoked when no longer needed or when alternative compliant solutions become available.

14. Compliance and Enforcement

Compliance with this Policy is mandatory. Violations may result in disciplinary action up to and including termination of employment or contract, and may also result in legal action where applicable. Third parties who violate this Policy or applicable access requirements may be subject to contractual remedies, including suspension of access and termination of agreements.

Compliance shall be assessed through periodic internal reviews, technical verification activities, and audits. Noncompliance shall be recorded, remediated, and reported through the Organization’s ISMS governance processes.

15. Related Policies and Supporting Documents

This Policy is supported by, and shall be read in conjunction with, the Organization’s Information Classification and Handling requirements, Identity and Access Management procedures, Privileged Access Management procedures, Authentication and Credential Handling requirements, Physical Security requirements, Logging and Monitoring requirements, and applicable HR onboarding/offboarding processes.