ACCESS TO INFORMATION TECHNOLOGY POLICY

PURPOSE

This directive establishes the requirements for managing both physical and logical access to Information Technology (IT) applications, ensuring the security, confidentiality, integrity, and availability of systems and data. It outlines the responsibilities, controls, and processes necessary to safeguard IT applications from unauthorized access, mitigate risks, and comply with relevant regulations and standards.

OBJECTIVE

The objective of this policy is to establish and enforce comprehensive controls over both **physical access** (to IT infrastructure) and **logical access** (to IT applications and systems) in order to:

1. **Protect Information Security**: Safeguard the confidentiality, integrity, and availability of sensitive data and IT systems by preventing unauthorized access, misuse, or theft.
2. **Ensure Compliance**: Adhere to legal, regulatory, and industry-specific requirements for access control.
3. **Mitigate Risks**: Reduce the risk of security incidents, including unauthorized access, data breaches, and operational disruptions, by implementing effective access management practices.
4. **Define Access Responsibilities**: Clearly outline the roles and responsibilities of personnel involved in managing and overseeing both physical and logical access to IT resources.
5. **Enforce the Principle of Least Privilege**: Ensure that users and systems only have access to the information and resources necessary for their specific roles, minimizing the potential for misuse or accidental disclosure.
6. **Facilitate Audit and Monitoring**: Establish processes for logging and monitoring access to IT systems and infrastructure, enabling the detection of unauthorized activities and ensuring accountability.
7. **Maintain Business Continuity**: Ensure that access controls are maintained in a way that supports the organization’s operational needs while minimizing potential threats to its IT environment.

By achieving these objectives, the policy aims to foster a secure, compliant, and efficient IT environment that supports organizational goals while safeguarding against external and internal security risks.

POLICY

This policy applies to all employees, contractors, vendors, and other authorized users who interact with the organization's IT applications, including both physical access to the hardware infrastructure and logical access to application systems, networks, and data.

DEFINITIONS

Physical Access: The ability to physically access IT hardware, servers, workstations, networking equipment, and data storage devices.

Logical Access: The ability to access IT applications, systems, and data through authentication and authorization mechanisms such as usernames, passwords, tokens, or biometric data.

Access Control: The process of granting or denying access to IT systems, networks, and applications based on security policies.

PHYSICAL ACCESS CONTROL

To protect against unauthorized physical access to IT resources, the organization will implement the following controls:

- **Access Authorization**: Only authorized personnel will be permitted to access sensitive or restricted areas housing critical IT infrastructure, including server rooms, and network equipment locations.
- **Physical Barriers**: Areas containing critical IT assets will be secured by physical barriers such as a lockable door.
- **Access Logging**: All physical access to restricted areas must be logged. Logs should include details such as the identity of the individual, time of entry and exit, and the reason for access.
- **Visitor Management**: Visitors must be accompanied by an authorized staff member and access to restricted areas should be monitored. Visitor logs must be maintained for auditing purposes.

LOGICAL ACCESS CONTROL

To prevent unauthorized logical access to IT applications and systems, the organization will implement the following controls:

- **User Authentication**: Access to IT systems and applications will require the use of secure authentication methods such as passwords or multi-factor authentication (MFA).
- **Role-Based Access Control (RBAC)**: Users will be granted access to applications and data based on their role in the organization. Access rights should follow the principle of least privilege, ensuring users only have the necessary access to perform their job functions.
- **Access Reviews**: User access rights will be reviewed periodically to ensure that access is appropriate to the user's role and current job responsibilities. Any discrepancies will be addressed promptly.
- **Password Management**: Users must adhere to organizational password policies, including the use of strong passwords, periodic password changes, and the prohibition of password sharing.
- **Session Monitoring**: All application and system access sessions will be monitored and logged to detect any unauthorized access attempts or suspicious activity.
- **Remote Access**: Access to systems and applications from remote locations will be secured through Virtual Private Networks (VPNs), encrypted communication channels, and other secure methods to prevent interception or unauthorized access.
- **Segregation of Duties**: Critical processes will require the involvement of multiple individuals to ensure no single user has access to both the authorization and execution of sensitive tasks.

ACCESS MANAGEMENT RESPONSIBILITIES

a. **IT Security Team**: Responsible for the implementation, monitoring, and maintenance of physical and logical access controls. This includes managing access permissions, reviewing logs, and ensuring compliance with security policies.

b. **HR Department**: Responsible for notifying the IT department of new hires, role changes, or terminations to facilitate timely access changes.

c. **Managers and Supervisors**: Responsible for ensuring that access to IT applications is granted based on the user's job role and that access rights are updated as necessary.

d. **End Users**: Responsible for following organizational policies and best practices for securing their access credentials and reporting any suspicious activity.

INCIDENT RESPONSE AND BREACH MANAGEMENT

In the event of a physical or logical access breach, the following actions will be taken:

- **Incident Reporting**: All suspected security incidents involving unauthorized access should be immediately reported to the IT Security Team.
- **Investigation**: The IT Security Team will investigate the breach to identify the scope, method, and potential impact of the unauthorized access.
- **Containment**: Immediate steps will be taken to contain the breach, such as disabling accounts, changing passwords, and restricting physical access.
- **Remediation and Recovery**: Corrective actions will be implemented to prevent further incidents, such as tightening access controls, patching vulnerabilities, and conducting employee retraining.
- **Notification**: If required by law or regulation, affected individuals and relevant authorities will be notified about the breach.

COMPLIANCE & AUDITING

Regular Audits: Regular audits of both physical and logical access controls will be conducted to ensure compliance with this directive and identify areas for improvement.

STATUTORY ENVIRONMENT

Local Government Act 1995

Record of Policy Review						
Version	Author	Council Adoption	Resolution	Reason for Review	Next Review Date	CEO Signature
01	Tricia Brown	27/02/2025	112 - 24/25	New Policy	Feb 27	Natalie Ness.