Physical Access Policy

Policy to govern physical access controls within the Microlink premises.

# Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change |
| 0.1 | 02/03/2022 | David Henderson | Initial draft to combine multiple password policy items into a central policy |
| 1.0 | 30/09/2022 | David Henderson | Initial publish |
|  |  |  |  |
|  |  |  |  |

**Document Owner IT**

# Introduction

Facilities and Internal IT are responsible for managing access in and around the organisation. The following key business objective can be fully or partially met using physical access controls:  
Staff safety by not allowing unknown members of the public into the operational areas of the building where staff reside. Protect against losses by restricting access to high value areas to only those that require it. Improve information and data security and privacy by only allowing those authorised to access data processing facilities to do so. The system also aids track clocking information for presents and punctuality.

With the organisation growing organisation wide familiarity of staff is reducing and continuing to do so. It is important to be able to quick and safely identify staff, Contractors and Visitors. Ensure that data and staff security requirements, and health and safety requirements are always met.

# Policy Objectives

* 1. This policy is to identify the requirement for staff, contractors, and visitors with regards to physical door access and ID and Key management.

# Definitions

|  |  |
| --- | --- |
| *Definition* | *Meaning* |
| Physical Access keys: | ID cards, Electronic Keys, mechanical Keys Fobs, MFA devices these are physical items that permit access to secure location or lock boxes. |
| Access controls equipment | All equipment that is used to impede or deny physical access to an area such as an Electronically locked door, Barrier, Turn style, Mechanical bollards. |

# Applicability

This policy applies to all activities where you are required physical access to any location within the building.

You request a visitor to attend the premises.

# controls

## Access cards/ ID badges

ID cards and passes can help identify unfamiliar faces. Identify visitors by staff and identify staff by visitors. ID passes also provide a mechanism to electronically identify a user, allowing or denying them access to an area. Because the ID card can be tracked around the premises, they are also used in the event of an evacuation to identify your last known location and generate a roll call of who have been in the building. Due to access, they grant, and the health and safety demand placed on the system various controls are required to ensure they are used correctly

* + 1. Employees
       1. All employees must be issued an ID card. (For identification and security purposes)
       2. All cards must use unique assigned access ID. (To reserve integrity of event data)
       3. All cards must be uniquely identifiable visually and digitally including Full Name, and Photo that marks a true resemblance to the card holder. This is to identify and deter misuse (imposter, falsify clocking information, and sharing cards)
       4. It is prohibited to share use of and issued Access token. (for security, fraud ie clocking info and health and safety reasons)
       5. Must identify the holder as an employee of Microlink (use the **BLUE** design for security reasons)
       6. It is the employee’s responsibility to ensure ID badge kept on display. Those who frequently forget their ID card or fail to wear it on display will be subject to disciplinary action.
       7. All employees responsible for informing IT department of any change to number plates ownership that has been registered with IT (registering number plates is not mandatory)
    2. Contractors
       1. Long term contractors or contractors that visit the site regularly may be issued an ID card with approval from CEO, MD, or COO.
       2. All cards must be uniquely identifiable including Full Name, and Photo that marks a true resemblance to the card holder. This is to identify and deter misuse (imposter and sharing cards).
       3. It is prohibited to share use of and issued Access token.
       4. Must identify the holder as a contractor of Microlink (use the **RED** design).
       5. It is the contractor’s responsibility to wear their ID badge on display. Those who frequently forget their ID card or fail to wear it on display may be asked to leave the premises until the card can be presented.
       6. Contractors are only authorised to enter the premises to carry out their business duties.
    3. Visitors
       1. Are not to be issued access tokens but instead paper-based ID.
       2. Must not be left unattended at any time (excluding public areas, Smoking area, and Canteen)
       3. Visitors are not permitted into restricted areas or where there is sensitive and or confidential records or sensitive equipment.
          1. Representatives of regulatory bodies and stakeholders may be exempted.
       4. Visits are only approved during working hours.
       5. Actions of visitors are the responsibility of the staff member they are visiting.

# Access control

* 1. Where Access tokens are provided and access request changes, (Grant, Update, Revoke) must be logged and recorded (IT ticket) on a per request basis.
  2. Approval must be granted by the relevant area owner. The area owner is listed in the “Doors System overview.docx” (system production/Doors)

# Access Key restrictions.

To ensure security is maintained access keys must be protected and handled correctly. Failing to handle access keys correctly could result in unauthorised access to Microlink premises and systems, consequently enabling theft of property or data, damage to property or systems or introduction of malicious equipment or items. There for the following restrictions apply.

* 1. Physical access Keys must be kept stored in a secure location.
     1. Including physical access Keys taken offsite.
     2. Locked Cars and externally located lock boxes are prohibited from use.
     3. Physical access keys must be kept on your person when not being securely stored.
  2. All physical access Keys must be returned when:
     1. Employment is terminated.
     2. Employment role changes and possession of physical access keys is no longer required.
  3. If physical access keys are lost or stolen:
     1. Internal IT must be informed immediately.
     2. Facilities Must be informed immediately.
     3. Incident must be raised using the incident management system.

# Access control equipment restriction.

To ensure adequate security protections are in place and the ability continually monitor the operational effectiveness, policy compliance, control effectiveness and ensure security requirement. Several restrictions regarding access control equipment are required.

* 1. All access controls that are situated to protect a restricted high value areas or data processing area must:
     1. Have an audible alarm that sounds when:
        1. The door is forced open.
        2. The door is held open.
     2. Create a log of the event when:
        1. The door is forced open.
        2. The door is held open.
        3. An access badge is used that does not have adequate permission.
        4. Event that unlocks all doors occurs (ie Fire alarm)
     3. All access controls that are situated to protect Server room/ Datacentres must also:
        1. Have CCTV covering the entrance.
     4. Where reasonably practicable controls must be in place to deter or prevent:
        1. Tailgating. The action of someone following someone else through an access control without presenting their Electronic Key to the reader.
        2. Pass back. The action of someone passing their electronic key back to provide another access.
     5. Access controls must follow a minimum standard build practice to ensure safety, monitoring and alarming. See “New Door installation Specification” document for more information.

# Exceptions.

* 1. Temporary Cards are not required to be visually identifiable form of photo ID.
  2. Emergency services are exempt when responding to emergency.

# Failure to comply.

Any violation of this policy should be brought to the attention of the Head of IT and the Information Security Manager, who will work with the relevant department heads or appropriate individuals to rectify the problem.

# Access Review Auditing

Regular access review audits are carried out to ensure the effectiveness of the physical access system, ensure the effectiveness of the Policy and procedures and instil confidence with stake holder regarding physical security.

* 1. Access review Audits must be carried out at least every 3 months with the relevant area owners.
  2. All access reviews must include all active accounts where any form of access is granted.
  3. Each individual account must be scrutinised during the audit and separate approval for each account must be recorded.
  4. All audits must be recorded.