Physical Security Policy

Nexelus

Purpose

The Physical Security Policy establishes requirements to ensure that Nexelus' information assets are protected by physical controls that prevent tampering, damage, theft, or unauthorized physical access. This policy defines the following controls and acceptable practices:

- Definition of physical security perimeters and required controls.
- Personnel and visitor access controls
- Protection of equipment stored off-site.

Scope

This policy applies to all Nexelus physical facilities and users of information systems within Nexelus, which typically include employees and contractors, as well as any external parties that have physical access to the company's information systems. This policy must be made readily available to all users.

Background

It is the goal of Nexelus to safeguard information both virtually and physically, as well to provide a safe and secure environment for all employees. As such, access to the Nexelus facilities is limited to authorized individuals only. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Nexelus' facility.

Roles and Responsibilities

Network and Admin Manager are responsible for establishing and monitoring this policy.

Policy

General

- Physical access to Nexelus facilities is restricted.
- Only pre-authorized personnels are allowed to enter secure facilities if applicable (such as server rooms, data centers, labs).
- All employees must follow physical security requirements and procedures documented by facility management.
- On-site visitors and vendors must be always escorted by a Nexelus employee while on premise.

- All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Nexelus' facility.
- Building security, such as fire extinguishers and detectors, escape routes, floor warden responsibilities, shall be maintained according to applicable laws and regulations.

Access Requirements

- Physical access is restricted using badge readers, keys or smart locks that restrict access.
    - Restricted areas and facilities are locked when unattended (where feasible).
    - Only authorized workforce members receive access to restricted areas (as determined by the Security Officer).
    - Access and keys are revoked upon termination of workforce members.
    - Workforce members must report a lost and/or stolen key(s) or badge(s) to his/her manager, local Site Lead, or the Facility Manager.
    - The Facility Manager or designee is responsible to revoke access to the lost/stolen badge(s) or access key(s), and re-provision access as needed.
    - The Facility Manager or designee facilitates the changing of the lock(s) within 7 days of a physical key being reported lost/stolen.
- Visitor access requires additional controls.
    - Normally the company does not have visitors in case a visitor arrives at the office then the visitors sign a visitor’s log indicating date and time in/out, organization represented (if applicable), purpose of visit, and company point of contact. visitors must be accompanied by authorized personnel.
- Delivery and Loading areas.
    - Access to delivery and loading areas from outside of the facility will be restricted to only identified and authorized personnel.
    - Such areas will be designed to ensure that access to other parts of the facility is restricted.
    - Incoming material must be appropriately inspected for any discrepancies, issues, or potential threats, and must be registered in accordance with *Asset Management* procedures.
    - When possible, incoming, and outgoing shipments will be physically segregated.
- Enforcement of Facility Access Policies
    - Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
    - Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
    - Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from Nexelus.
- Workstation Security
    - Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
    - All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Control Policy.
    - All workstations must be secured by screen saver and password security.

    - All workstations purchased by Nexelus are the property of Nexelus and are distributed to personnel by the company.

Building Standards per Location

Standards

- A security perimeter must be defined and established to protect areas containing sensitive data and critical information processing facilities.
- The walls, ceilings and floor of any secure area must be of the same strength.
- Windows and doors have locks, and all entry points are secured by either keys or access control mechanisms and have cameras for additional monitoring as needed.
- Spaces around the perimeter or building access areas are monitored with CCTV or security patrols.
    - CCTV recordings need to be kept for at least 3 months.
- Keys to all secure or public areas housing IT equipment (including wireless access points, gateways, and more) must be protected in a centralized fashion.
- Offsite backup locations are physically secure for backups and the security measures are reviewed at least annually.

Location(s)

- **New York** Office:
    - The building is unlocked at least during normal business hours.
    - After hours the building is secured, and access is granted to personal card for entry.
    - The office is secured and requires an access card for entry.
    - ~~o~~ All sensitive data and applications are hosted in cloud. There is no need for extra security for Network Rooms. The server rooms are kept locked with access key assigned to Network Administrator.
- **Islamabad** Office:
    - The building is unlocked during normal business hours.
    - After hours the building is secured and requires an access card for entry
    - The office is secured and requires an access card for entry for after-hours access.
    - All server rooms are secured 24/7 and require an access card for entry.
- All server rooms are secured 24/7 and require an access card or key for entry.

Data Center Security

Physical and environmental security of data center is ensured by Azure, including all the controls listed in the sections below:

Asset Security

The following factors will be considered and implemented, as applicable per risk assessments, and in conjunction with the following policies: *Information Security Policy*, *Asset Management Policy*, *Data Protection* and *Data Classification*.:

External/Environmental Threats

Reasonable measures will be taken to protect company assets.

-

Backup Power

- All mission critical information assets are hosted by the cloud provider, Azure.