**Purpose and Scope**

The Physical Security Policy specifies the requirements for physically protecting assets and their data via physical controls and safeguards. Physical security is the first line of defense in information security, and without physical protections, virtual protections offer minimal security for assets and data. [Organization Name] maintains reasonable steps to ensure that its facilities, information systems, and data are accessed only by authorized personnel or authorized third party visitors to prevent unauthorized access, damage, theft, and interference. All physical security requirements are applicable to both remote and in-office work. Key aspects of physical security include: perimeter and border security, entry controls, visitor management, restricted areas, equipment protection and maintenance, awareness and training, and risk management.

**Perimeter and Border Security**

[Organization Name] facilities will be secured via external locked doors. Radicl facilities will be monitored via personnel, security cameras, and/or other mechanisms to detect potential security threats and respond to alerts.

**Entry Controls**

[Organization Name] requires employees and applicable contractors to utilize access cards/keys and/or PIN codes to unlock external doors throughout all business hours. For facilities not utilizing an access card system that tracks individual employees entering or exiting the premises, authorized personnel shall sign in/out using an authorized personnel sign in sheet. For facilities that have a security desk at the point of initial external access, external doors can be left unlocked as long as 1) employees and/or contractors authenticate prior to internal access via key/badge and 2) visitors are required to sign-in at the security desk prior to internal admittance.

All physical entry records for authorized personnel shall be stored for at least 12 months.

**Visitor Management**

All visitors must be escorted and monitored by an authenticated [Organization Name] employee.

All visitors shall sign in and out at the primary physical entry point utilizing the “Visitor Log”. A record of all visitor logs shall be stored for at least 12 months.

**Restricted Areas**

Only authorized personnel shall be allowed entry into restricted areas. Restricted areas may include:

* Personal, confined offices
* Network closets
* Power & utilities closets
* Server rooms (as applicable)
* Equipment storage rooms
* Operational areas/rooms

Restricted areas must be secured via access badges/keys/PIN codes or security personnel. All restricted areas and authorized individuals will be listed in the “Physical Access Authorized Personnel” form.

**Equipment**

The following types of protection and monitoring equipment should be maintained at all times:

* Power utilities (e.g. generators, UPS)
* HVAC systems, including environmental sensors (thermometers and humidity sensors)
* Fire suppression systems
* Network, power, and telecommunications cabling
* On-premise servers and desktops (as applicable)
* Physical data backups

[Organization Name] must securely store/protect the aforementioned equipment/assets from physical threats via proper access controls.

[Organization Name] shall maintain awareness of necessary maintenance schedules for the aforementioned equipment/assets. Maintenance should occur accordingly to prevent the failure of any of the aforementioned assets. Any third party/maintenance company that has access to a [Organization Name] facility (e.g. night cleaning company) must receive security clearance from management and must follow all applicable parts of the security policies. Maintenance to and external movement of physical security components should be documented and tracked accordingly.

**Physical Access Devices**

[Organization Name] shall track and manage all physical access devices for all facilities. An annual audit shall be conducted on the inventory to verify all access devices are accounted for. All physical access devices that are assigned to authorized users shall be documented in the “Physical Access Device Inventory” form.