**COMPANY: Physical Access Policy**

General

* The use of physical security systems is subject to all existing laws, including but not limited to building and fire safety standards.
* All restricted facilities used by the (Company) must have documented and controlled physical access.
* Depending on how vital or crucial to the Company any Information Resource facility is, it must be physically protected.
* Only (Company) support staff and contractors whose job duties necessitate access to that facility may be permitted access to Information Resources facilities.
* Every facility entry that could be used by unauthorized people needs to be guarded.
* To lower the risks from environmental dangers, hazards, and opportunities for unlawful access, taking precautions to reduce the risk of potential physical and environmental threats, carefully positioning information processing facilities handling confidential information to minimize the chance of unauthorized users viewing that information, and monitoring environmental conditions like temperature and humidity for anything that might negatively affect how those facilities operate.
* Equipment needs to be safeguarded from blackouts and other disturbances brought on by utility faults.
* Locations with restricted access must not have any signs or other indicators of the location's significance.
* A sign-in/sign-out log will be used to keep track of visitor access at all Information Resources locations that permit visitors.
* Depending on how crucially the Information Resources are to be secured, card access records and visitor logs for information resource facilities must be preserved for routine examination.
* Visitors must always be escorted by authorized employees while in restricted sections of Information Resource facilities.
* Physical facility management staff for Information Resource must periodically analyze access logs and visitor logs for the facility and look into any suspicious access.

Access Cards

* The approval of physical security staff is required as part of the process for giving card and/or key access to Information Resource facilities.
* The proper access and non-disclosure agreements must be signed by each person who is given access to an information resource facility.
* Cards may not be transferred to another person without first returning them.
* People who change roles within the company or lose their connection to it must have their access cards and/or keys removed by physical security staff.
* Physical security professionals are required to periodically check card and/or key access privileges for the facility and remove access for anyone who no longer need it.

Utility Systems

* The facility's utility systems must all be defined, documented, and include comprehensive maintenance requirements.
* To provide an audit record of all operations, maintenance and testing must be carried out in line with the manufacturer's standards.
* Unauthorized access must be prevented to utility systems.
* Utility systems must be set to sound an alarm when they malfunction.
* To ensure functionality, emergency power, lighting, and suppression systems must be installed and frequently checked.
* Critical utilities must be configured in a redundant manner to ensure continued functionality.

Loading Docks

* Documentation of the delivery and receipt of packages is required.
* Delivery sites must be gated off from the general public and secured.
* When inside doors are open, the delivery area's external doors must be locked.
* When unattended, delivery locations must be locked. Within delivery areas, unapproved individuals must always be escorted.
* Delivery locations must be fully covered and secured by surveillance cameras.
* Before being moved to internal areas, incoming deliveries must be registered, separated, and checked for signs of tampering.
* Physical security officers must be notified immediately of any evidence of tampering.