PHYSICAL & ENVIRONMENTAL SECURITY POLICY

Purpose

This policy defines the requirements for protecting Company's information and technology resources from physical and environmental threats in order to reduce the risk of loss, theft, damage, or unauthorized access to those resources, or interference with Company's operations.

Scope

This policy applies to all Departments that use Company's information technology resources to create, access, store or manage Data to perform their business functions.

Uninterruptable Power Supply (UPS)

A device designed to provide power, without delay, during any period when the normal power supply is incapable of performing acceptably.

Implementing Procedures

Physical Security

Network wiring and equipment – Network wiring and equipment rooms and cabinets must be locked when unattended with access limited to authorized personnel (typically network support staff) and visitors escorted by said authorized personnel. Other network cabling and devices should likewise be physically secured where feasible.

Office doors – All office doors should remain locked after hours or when offices are unattended for a prolonged period of time.

Environmental Security

Electrical power – Electrical power for servers hosting enterprise and departmental services must be protected by uninterruptable power supplies (UPS) to ensure continuity of services during power outages and to protect equipment from damage due to power irregularities. Each UPS have sufficient capacity to provide 04:00 hours of uptime to the systems connected to it. Systems hosting confidential data should also be protected with a standby power generator where feasible.