Version: [Version Number] Classification: Internal



[Company]

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

Security of physical locations and environments

Last Reviewed: [Last Reviewed] Page 1 of 12

Version: [Version Number] Classification: Internal



Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

Last Reviewed: [Last Reviewed] Page 2 of 12

箫

Version: [Version Number] Classification: Internal

Document Contents Page

Document Version Control	2
Document Contents Page	3
Purpose	5
Scope	5
Physical and Environmental Security Policy	5
Principle	5
Physical Security Perimeter	5
Secure Areas	6
Employee Access	7
Visitor Access	7
Delivery and Loading Areas	8
Network Access Control	9
Cabling Security	9
Equipment Siting and Protection	10

Last Reviewed: [Last Reviewed]

7

Version: [Version Number] Classification: Internal

Policy Compliance......12



Last Reviewed: [Last Reviewed] Page 4 of 12

Version: [Version Number] Classification: Internal

*

Purpose

The purpose of the policy is to prevent unauthorized physical access, damage and

interference to the organization's information and information processing facilities.

Scope

Physical and Environmental Security Policy

Principle

Physical and environmental security policy is built on the principle of exceeding Health

and Safety regulation whilst protecting the most sensitive physical assets based on

risk.

Physical Security Perimeter

The physical perimeter of the building or site containing information processing

facilities is physically sound. The exterior roof, walls and flooring of the site are of solid

Last Reviewed: [Last Reviewed]

Page 5 of 12

Version: [Version Number] Classification: Internal



Secure Areas

Access rights to secure areas are regularly reviewed and updated and revoked when necessary.

Access to secure areas defaults to deny.



Last Reviewed: [Last Reviewed] Page 6 of 12



Version: [Version Number] Classification: Internal

Photographic, video, audio, or other recording equipment, such as cameras in mobile devices is not permitted in secure areas unless authorized.

Employee Access

Employee access is based on least privilege providing access based on role.



Visitor Access

Visitors are allowed unfettered access to the public areas.

Last Reviewed: [Last Reviewed] Page 7 of 12

Version: [Version Number] Classification: Internal



Delivery and Loading Areas

Access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel.



Page 8 of 12 Last Reviewed: [Last Reviewed]

Version: [Version Number] Classification: Internal



Network Access Control

Physical access to networking equipment is restricted which includes wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

Cabling Security

Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference, or damage.

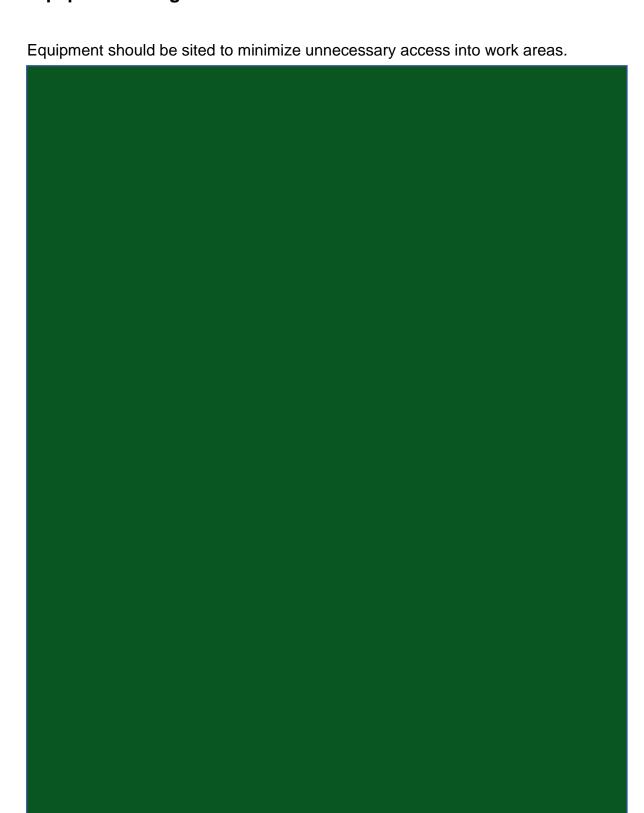


Last Reviewed: [Last Reviewed] Page 9 of 12

Version: [Version Number] Classification: Internal



Equipment Siting and Protection



Last Reviewed: [Last Reviewed] Page 10 of 12

Version: [Version Number] Classification: Internal



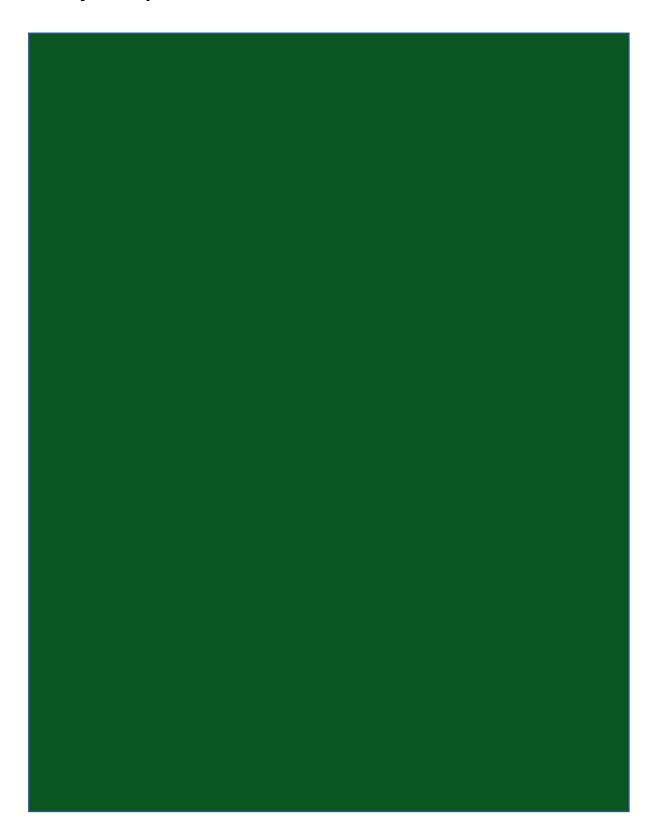


Last Reviewed: [Last Reviewed] Page 11 of 12

Version: [Version Number] Classification: Internal



Policy Compliance



Last Reviewed: [Last Reviewed] Page 12 of 12