[Company]

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

Security of physical locations and environments

Document Version Control

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

Document Contents Page

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

Secure Areas

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

Access to secure areas defaults to deny.

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.

Delivery and Loading Areas

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

Network Access Control

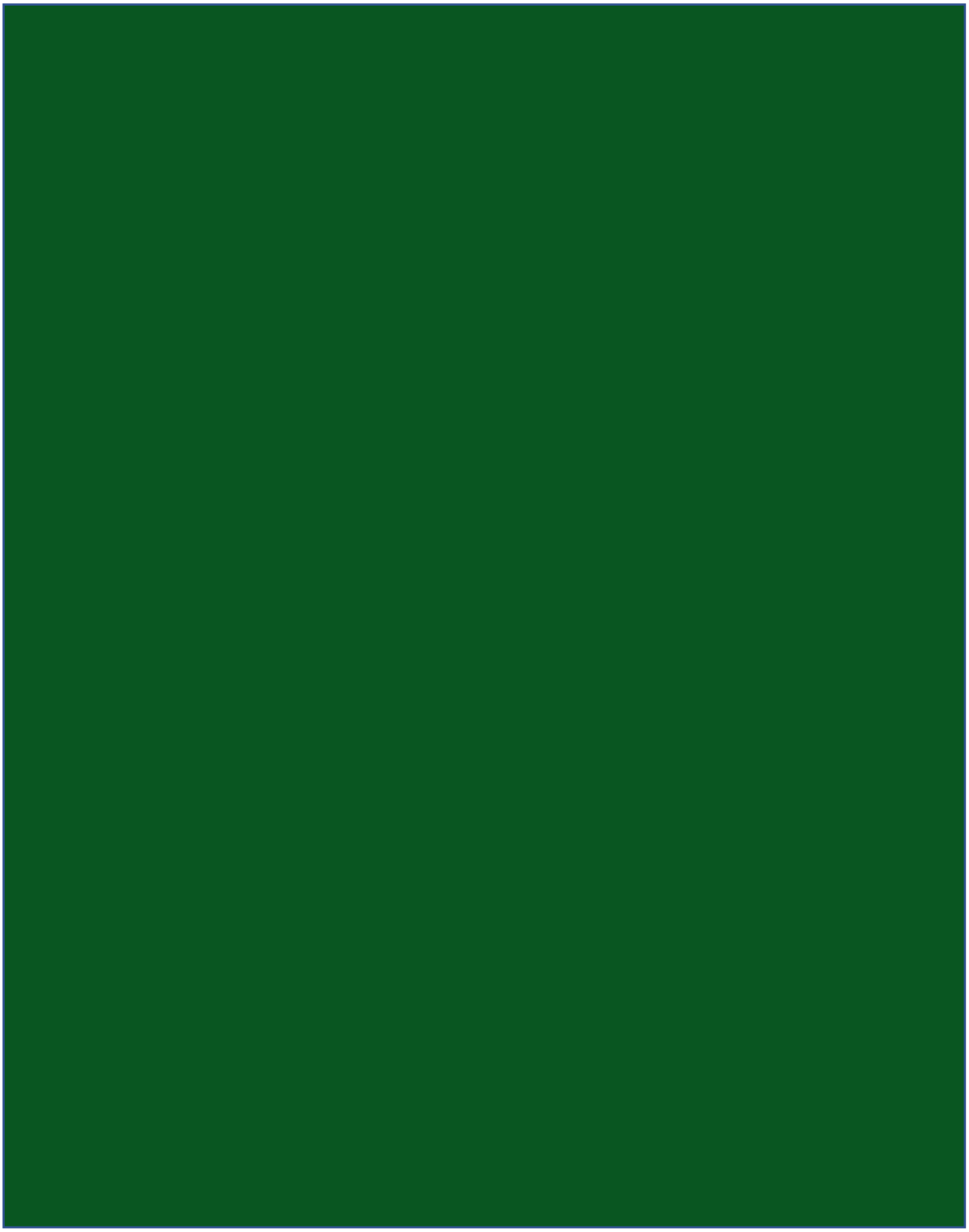
Physical access to networking equipment is restricted which includes wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

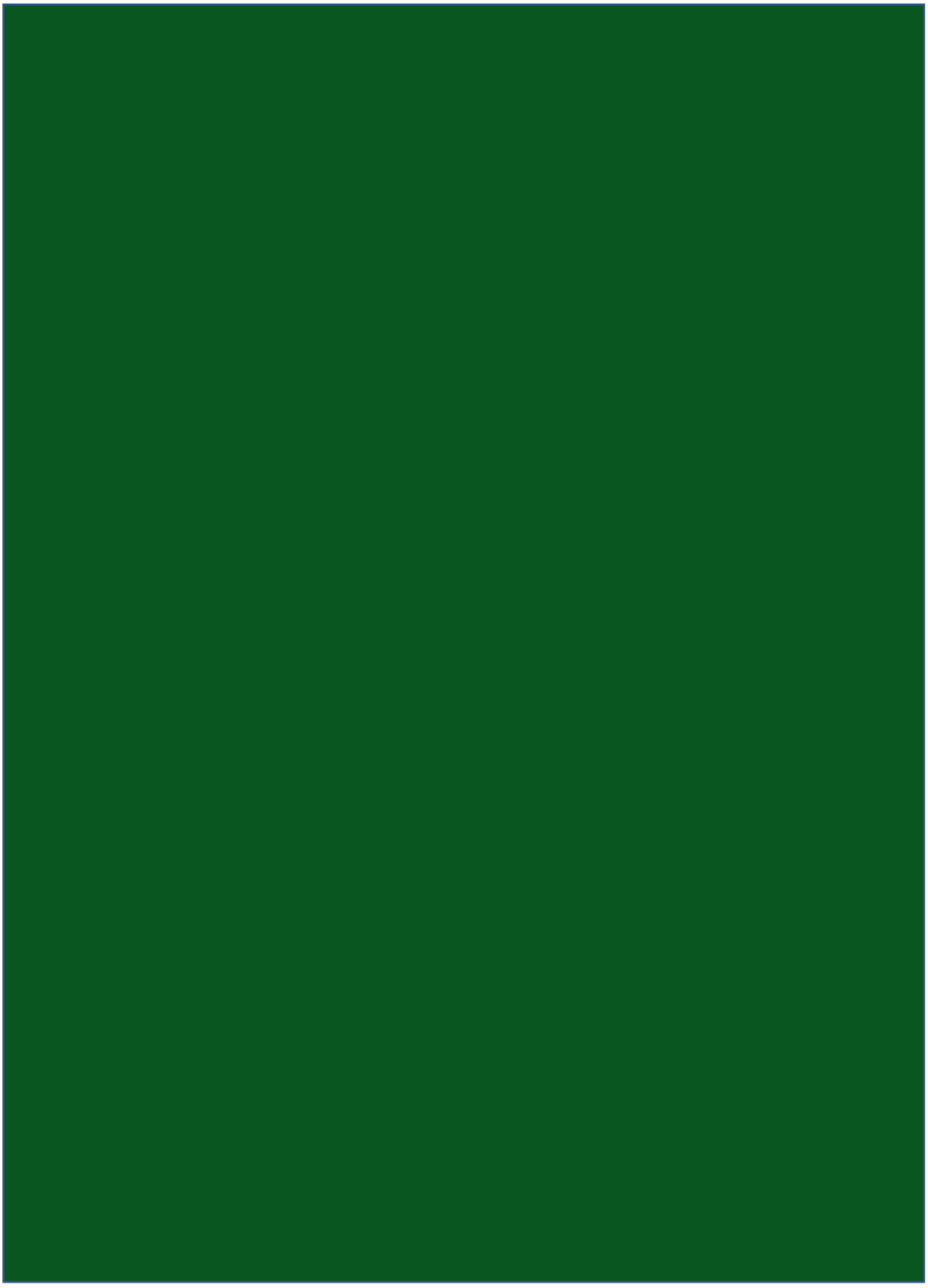
Cabling Security

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

Equipment Siting and Protection

Equipment should be sited to minimize unnecessary access into work areas.





Policy Compliance