Your Company Here

Generic Office Facility Access Policy

Document Number

1 PURPOSE

This policy outlines the policies and procedures regarding access control for facilities where information systems reside, including publicly accessible areas at <COMPANY>. This policy also covers visitors and control and management of physical access devices.

2 SCOPE

2.1 This policy applies to all <COMPANY> employees, contractors, vendors, and agents that have access to the <COMPANY> facility and network.

3 APPLICABLE DOCUMENTS

3.1 Add applicable documents here

4 ABBREVIATIONS

ITM/SO - Information Technology Manager / Security Officer
ITS - Information Technology Services
IS - Information Systems
Wi-Fi - Wireless Fidelity
IT - Information Technology
PII - Privacy Information
CUI - Controlled Unclassified Information
FCI - Federal Contract Information

5 POLICY

5.1 GENERAL

5.1.1 Protecting <COMPANY> associates, facilities, assets, and data is of the utmost importance to <COMPANY> and to the work that is done. In today's digital world much effort is exerted in protecting digital assets on local computing networks and across the Internet. Physical security and control are just as important. Everyone working at the <COMPANY> office has a part to play in protecting people working at <COMPANY> and the assets and resources stored in <COMPANY> facilities. The protection also includes resources stored on <COMPANY> devices from harm, theft, destruction, and corruption.

5.2 MANAGEMENT RESPONSIBILITIES

5.2.1 The Information Technology Manager/Security Officer (ITM/SO) is responsible for:

- Add appropriate responsibilities.

Your Company Here

5.3 PHYSICAL SITE ACCESS

5.3.1 OVERALL SITE SECURITY

5.3.1.1 The ITM/SO is responsible for managing and maintaining the security the <COMPANY> office. This security responsibility includes the access card system that employees will use to enter the <COMPANY> facility.

5.3.1.2 Employees of the <COMPANY> will be permitted to enter the space during normal working hours.

5.3.2 ACCESS CARDS

5.3.2.1 Employees will receive an access card upon hire at <COMPANY>. Specify how the employees will enter the building and what would occur should the access card be lost or stolen.

5.3.3 PHYSCIAL KEYS

5.3.3.1 KEY-CODED LOCKBOXES

- Where additional access cards are stored and who is responsible for them.

5.3.4 <COMPANY> OFFICE DOORS

5.3.4.1 EMPLOYEE OFFICE DOORS

- Employees will be given a personal office for them to perform their day-to-day job duties. Employees are expected to always safeguard and protect the key to their office.
- When the employee is not present at the <COMPANY> office, the door to their office should remain locked. Failure to do so may result in theft of personal or company assets.

5.3.4.2 PUBLIC DOORS

- Define what a public door is.
- Describe any specifics that employees should be made aware of when using public doors.

5.4 VISITOR AND GUEST ACCESS

5.4.1 NON-EMPLOYEE ACCESS OVERVIEW

5.4.1.1 Non-employees are any people at <COMPANY> who are not currently on the payroll of <COMPANY>.

5.4.1.2 Provide more details if needed. Some additional information could be how to identify non-employees or if they need escorted through the building.

5.5 PHYSICAL EQUIPMENT AND ASSETS

5.5.1 Upon hire, employees will be given a computer, which may be a laptop or a desktop, for them to be able to perform their required job duties. It is the responsibility of the employee to protect the device and all sensitive company information that is contained on it. Failure to do so will result in disciplinary action up to and including termination of employment.

5.5.2 More information should be provided, such as what to do if the computer is lost or stolen.

5.6 INTERNET AND NETWORK ACCESS

5.6.1 Define who can use what network. If there is a Wi-Fi network, who has access to it?

Your Company Here

6 RECORDS

6.1 Records are maintained in accordance with <COMPANY PROCEDURE>.

Revision history

Rev.	Reason	Author	Date
A	RELEASE REASON	Company Employee	XX/XX/XX