January 1, 20XX

ABC Company

123 Main Street

Los Angeles, CA 90744

(800) ABC-COMP

[www.ABCCompany.com](http://www.ABCCompany.com)

Table of Contents

[I. Introduction 3](#_Toc49169288)

[A. Overview 3](#_Toc49169289)

[B. Risk Assessment 3](#_Toc49169290)

[C. Equipment 3](#_Toc49169291)

[D. Plan Updates 3](#_Toc49169292)

[II. Facility Overview 4](#_Toc49169293)

[A. Facility Information 4](#_Toc49169294)

[B. Business Operations 4](#_Toc49169295)

[C. Documentation 4](#_Toc49169296)

[III. Personnel Considerations 5](#_Toc49169297)

[A. Overview 5](#_Toc49169298)

[B. Personnel Controls 5](#_Toc49169299)

[C. Security Controls 5](#_Toc49169300)

[D. Mailing Handling 6](#_Toc49169301)

[E. Drills 6](#_Toc49169302)

[IV. Equipment Considerations 7](#_Toc49169303)

[A. Overview 7](#_Toc49169304)

[B. Equipment Controls 7](#_Toc49169305)

[C. Disaster Controls 7](#_Toc49169306)

[V. Environmental Considerations 8](#_Toc49169307)

[A. Overview 8](#_Toc49169308)

[B. Power Controls 8](#_Toc49169309)

[C. Heating and Air Conditioning System Controls 8](#_Toc49169310)

[D. Water Controls 9](#_Toc49169311)

[VI. Cabling Considerations 10](#_Toc49169312)

[A. Overview 10](#_Toc49169313)

[B. Power and Telecommunications Controls 10](#_Toc49169314)

[C. Sensitive or Critical Systems 10](#_Toc49169315)

[VII. Maintenance Considerations 11](#_Toc49169316)

[A. Overview 11](#_Toc49169317)

[B. Frequency 11](#_Toc49169318)

[C. Maintenance Controls 11](#_Toc49169319)

[VIII. Off-site Considerations 12](#_Toc49169320)

[A. Overview 12](#_Toc49169321)

[B. Off-site Controls 12](#_Toc49169322)

[IX. Equipment Disposal/Re-use Considerations 13](#_Toc49169323)

[A. Overview 13](#_Toc49169324)

[B. Disposal/Re-use Controls 13](#_Toc49169325)

[Appendix A – Supporting Documents 14](#_Toc49169326)

[Appendix B – Receipt and Acknowledgement 15](#_Toc49169327)

# I. Introduction

### A. Overview

This Facility Security Plan (Plan) describes the methods, procedures, and measures used to establish security measures and prevent loss, damage or compromise of assets and interruption to business activities.

This Plan is established to help ensure the organization can prevent loss of services and protect the integrity, availability and confidentiality of information. This Plan provides a well-defined and organized approach for implementing and maintaining controls that reduce threats to facilities and physical environment.

### B. Risk Assessment

A risk assessment and risk analysis was performed to assess security risks, likelihood of events, and impact on our organization. The risk assessment identified risks to equipment, facilities, data, communications, servers, and many other types of Information Resources. The risk analysis identified preventive, detective, and corrective controls that treat risks.

### C. Equipment

Equipment should be physically protected from security threats and environmental hazards.

Protection of equipment, including that used off-site, is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. Special controls are required to protect against hazards or unauthorized access, and to safeguard supporting facilities.

### D. Plan Updates

This Plan should be reviewed and updated on an annual basis. This Plan is reviewed, maintained, and updated by the VP of Corporate Security and Safety.

# II. Facility Overview

### A. Facility Information

**ABC Company is located at the address on the cover page of this Plan. The building is a mixed-use, multi-tenant facility. Current floor plans are on file with the Facilities Department.**

### **B. Business Operations**

**Number of employees, contractors, and daily visitors on-site at this facility: [ list quantity ]**

**General functions performed at this facility: Administrative**

### C. Documentation

Policies and procedures should specify all physical security components that require documentation. Procedures should specify documentation of repairs and modifications to the physical components of a facility that are related to security (e.g. hardware, walls, doors, locks, cameras, alarms, etc.).

Procedures and related documentation should identify when special circumstances dictate repairs or modifications to physical security components are required. For example, when Staff with special privileges are terminated.

# III. Personnel Considerations

### A. Overview

**ABC Company is located at the address on the cover page of this Plan. The building is a mixed-use, multi-tenant facility. Current floor plans are on file with the Facilities Department.**

### **B. Personnel Controls**

A risk assessment and risk analysis should evaluate personnel related risks. The risk analysis and risk assessment should identify personnel related controls.

Documented procedures should control and validate a person’s access to facilities is based on his/her role or function, including visitor control, and control of access to software programs for testing and revision. Procedures should control and validate a Staff member’s access to facilities and consider guards, ID badges, key cards, etc. Procedures should specify visitor controls such as visitor sign in, wearing of visitor badges, escorting by authorized personnel, etc. On a periodic basis, management should review of the list of individuals with physical access to sensitive facilities.

**Vehicles:**

* **Public – public parking is available in an unsecured parking lot. Lighting is available during evening hours.**
* **Employees – employees may park in a restricted parking lot available only to employees. The employee parking lot is restricted by means of attendant and gate. Numbers, not names or departments, are used to identify restricted spaces.**

**Entrances:**

* **Entrances – where possible, minimize the number of public entrances.**
* **Screening – consider the use of metal detectors and X-ray machines at public entrances.**

**As appropriate, security screening may also be performed at employee entrances.**

**Registration**

* **Visitors – visitors and other Staff (e.g. consultants, temporaries) without organization identification badges must sign in at the registration desk and show proof of identification.**
* **Employees – employees with identification badges may by-pass the registration desk.**

**Restricted access**

* **Visitors – visitors and other Staff must be escorted by organization personnel while on organization premises.**
* **Employees – employee identification badges are used as access cards. Each access card has been pre-programmed with appropriate rights that permit access to selected locations within the facility.**

**Shipping and receiving**

* **Segregated – shipping and receiving areas should be segregated from the main facility.**
* **Access – personnel in this area should not have direct access to other organization facilities.**

### **C. Security Controls**

**As appropriate, management should implement security protection controls such as locked doors, signs warning of restricted areas, surveillance cameras, alarms, ID badges, visitor badges, escorts, and security services/patrols of the facility. Property controls such as property asset tags and engravings may also be implemented.**

### **D. Mailing Handling**

**The Risk Assessment and Risk Analysis should evaluate other types of risks to facilities and Staff.** The risk analysis should consider controls that reduce risks related to the items listed below.

**Staff should be trained on how to identify suspicious mail. Examples include: mail with inappropriate or unusual labeling (e.g. excessive postage, misspelled words, no return address, titles with no name), or restrictive markings (e.g. “personal,” “confidential,” “do not x-ray”).**

**Staff should identify an unusual or inappropriate appearance (e.g. powdery substances felt through/on package, stains/discolorations, odors, excessive packaging material such as tape or string, bulky shape, ticking sounds, protruding wires, etc.).**

**Staff should be trained on how to handle suspicious packages and mail. Staff should not open, shake, show to others, or empty the contents of a suspicious letter or package. Instead, Staff should leave the letter or package where it is or gently place it on the nearest flat surface.**

**As appropriate, Staff should:**

* **Gently cover the letter or package using a waste basket or something similar.**
* **Shut off any fans or equipment in the area that may circulate the material.**
* **Alert others nearby to relocate to an area away from the suspicious item.**
* **Take essential belongings (e.g. cell phones, keys, and wallet) in case their return to the office is delayed.**
* **Immediately contact the Facilities Department.**
* **Leave the area and close the door to the space containing the suspicious letter or package.**

### **E. Drills**

**Drills and exercises simulate realistic and fluid situations where critical decision-making is learned and Staff is familiarized with emergency response procedures. Exercises help to broaden a deeper understanding of response procedures and identify areas for improvement.**

**Drills can range from discussion based (e.g. table-top, workshop) to full-scale exercises that involve all Staff. Staff should periodically participate in drills and tests of procedures. Examples include:**

* **Incident notification and activate appropriate alarms.**
* **Alarm response and building evacuation using exit routes posted throughout the facility.**
* **Business continuity testing of department and disaster recovery plans.**

# IV. Equipment Considerations

### A. Overview

Equipment should be located or protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access.

### B. Equipment Controls

Preventive, detective, and corrective controls should be considered and implemented to protect equipment and facilities:

* Threats – controls should be implemented to minimize the risk of environmental and physical threats that include unauthorized access, theft, damage, fire, water, smoke, dust, vibration, chemicals, electrical interference, electromagnetic radiation, and similar risks.
* Location – equipment should be located to minimize unnecessary access by authorized and unauthorized staff. The impact of terrorism, collateral damage, and similar threats should be evaluated when considering equipment location.
* Special needs – equipment that requires special security protection should be identified and isolated to reduce the likelihood of compromise.
* Personnel – Staff that implement, manage, and maintain equipment and facilities shall be properly trained.
* Prohibited activities – activities such as smoking, eating and drinking should be banned in or near Information Systems.
* Monitoring – environmental systems should be identified and monitored to ensure proper and continued delivery of services. Failover or redundant systems should be considered where there is a greater chance of downtime or impact on the organization.

### C. Disaster Controls

In the event of a disaster, the Business Continuity Disaster Recovery Plan identifies Emergency Action Facility Team procedures that address the salvage or replacement of equipment, network server room facilities, etc. Such procedures include:

* Working with Company management to identify options (repair existing or identify replacement) facilities.
* Working with outside vendors as appropriate for environmental, power and repair conditions.

# V. Environmental Considerations

### A. Overview

Information Systems and data centers have special environmental considerations. Equipment should be protected from power failures, air conditioning outages, fires, and similar types of threats.

### B. Power Controls

A reliable power source should be provided that conforms to equipment manufacturer requirements. Redundant and fail over systems can include:

* Power – power feeds from several suppliers.
* Generators – backup power generators.
* Uninterruptible Power – Uninterruptible Power Supply (UPS) on servers, critical networking equipment, and important workstations.

Power feeds. Power sources are generally classified into the following categories:

* Single feed from a single substation. This option presents the greatest risk as the power supply has numerous single points of failure.
* Single substation with two feeds. By having two separate feeds, the data center reduces the risk of a single line failure. However, this configuration only uses one substation as the power source.
* Dual substations. Two substations provide an additional level of redundancy over a single substation. This reduces the likelihood of a prolonged outage due to the failure of a single substation or its respective feed.
* Dual Feed. Power is supplied by two separate substations with a single independent feed from each. Power from both substations is fed directly into each of transformers located inside the building. There are no single points of failure and power loads within the facility are shared.

Generator. A backup generator can be used to provide power during prolonged power outages. If installed, generators should be installed by licensed professionals and regularly tested in accordance with the manufacturer’s instructions. An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period of time.

Uninterruptible Power Supply (UPS). A UPS uses batteries to provide power to critical systems for a limited amount of time. UPS systems can allows an orderly and controlled shut down of systems either manually or automatically. UPS systems should be tested on a regular basis to ensure they offer adequate capacity. Batteries should be replaced as needed.

Other power related considerations include:

* Equipment room emergency power switches should be located near emergency exits. In the event of an emergency, Staff can hit the switch to rapidly shut down power.
* Emergency lighting should be automatically activated in the event of a power failure.
* Lightning protection should be installed at all facilities. Lightning protection filters should be installed on all external communication lines.

### C. Heating and Air Conditioning System Controls

The required heating and/or cooling load is largely determined by the amount of floor space. In some instances, particularly in buildings with high ceilings, the volume of the space should be considered. In addition to measuring the area, consider heat transfer through walls, doors and roofs, lighting systems, IT equipment, and occupancy levels. Heating and air conditioning systems should be positioned so they are only accessible by authorized personnel and should be maintained per manufacturer requirements.

### D. Water Controls

The organization should evaluate water related risks and controls including:

* Dependence on water quality, quantity, and cost.
* Redundant water supply sources including water trucks.
* Miscellaneous factors that that may impact operations including water rights and legal obligations.

# VI. Cabling Considerations

### A. Overview

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

### B. Power and Telecommunications Controls

The following controls should be considered to protect against disruption in service or unauthorized interception of communications:

* Protection – where possible, cables to the facility should be underground.
* Network cabling – should be protected by conduit or other means. Where possible, routes should avoid public areas.
* Separation – power cables should be separated from communications cables to prevent interference.

### C. Sensitive or Critical Systems

Sensitive or critical systems may require additional controls including:

* Protection – armored conduit, locked closets, and boxes at inspection and termination points. Fiber optic instead of less secure Ethernet cabling.
* Redundancy – use of alternative routings or transmission media or solutions (e.g. wireless).
* Detection – periodic physical and electronic detection of unauthorized devices.

# VII. Maintenance Considerations

### A. Overview

Equipment should be properly maintained to ensure its continued availability, integrity, improved productivity, and reduced environmental impact. All equipment shall be maintained in an efficient state and in good working order. Maintenance logs shall be maintained and kept up-to-date.

### B. Frequency

The frequency and nature of maintenance activities should be determined through a risk assessment of the equipment that considers:

* Manufacturer recommendations.
* Requirements imposed by insurance policies.
* Intensity of use of the equipment.
* Operating environment (e.g. temperature, corrosion, weathering).
* User knowledge and experience.
* Risk to health/safety from any foreseeable failure or malfunction.

### C. Maintenance Controls

The following equipment maintenance controls should be considered:

* Equipment should be maintained in accordance with the manufacturer’s recommended service intervals and specifications.
* Only authorized maintenance personnel should carry out repairs and service equipment.
* Records should be kept of all suspected or actual faults and all preventive and corrective maintenance.
* Appropriate controls should be taken when sending equipment off-site for maintenance.

# VIII. Off-site Considerations

### A. Overview

Management must pre-authorize the use of equipment that will be used or hosted off-site of ABC Company’s premises. Where possible, the security provided should be equivalent to that for equipment used or hosted on-site at our location.

When making the decision to allow equipment to be used or hosted off-site, management should consider the risks of Staff working off-site.

### B. Off-site Controls

Where possible, the following controls should be implemented for off-site equipment:

* Equipment and media taken off the premises should not be left unattended in public places. Portable computers, tablets, media, etc. should be hand carried and not checked in luggage when traveling.
* Staff shall follow manufacturer instructions for protecting equipment (e.g. temperature, proximity to strong electromagnetic fields, etc.).
* Off-site controls (e.g. locking filing cabinets, Clear Desk Policy, access controls for Information Systems) should be applied.
* Adequate insurance should be in place to protect off-site equipment.

Security risks including damage, theft, eavesdropping, etc. may vary considerably between locations and should be taken into account when determining the most appropriate controls.

# IX. Equipment Disposal/Re-use Considerations

### A. Overview

Information can be compromised through careless disposal or re-use of equipment. Storage devices containing sensitive information should be physically destroyed or securely overwritten rather than using the standard delete function.

### B. Disposal/Re-use Controls

Equipment and media should be properly disposed of considering manufacturer and environmental requirements. The nature of disposal/re-use procedures should be determined through a risk assessment of the equipment/media that considers:

* Intended re-use of the device/media.
* Sensitive data stored on the device/media.
* Licensed software stored on the device/media.
* Compliance requirements.

Storage media (e.g. hard drives, flash drives, etc.) should be checked to ensure that any sensitive data and licensed software have been securely removed or overwritten prior to disposal or re-use.

Damaged storage devices containing sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

# Appendix A – Supporting Documents

This Plan is part of an overall approach to managing business and operational risks. Organization policies, plans, and forms provide additional direction and guidance. Examples of documents that support this Plan include, but are not limited to:

* Acquisition and Procurement Policy
* Business Continuity Policy
* Disaster Recovery Plan
* Disposal Policy
* Documentation Policy
* Hardware and Software Maintenance Policy
* Incident Response Plan
* Incident Response Policy
* Personnel Security Policy
* Physical Access Policy
* Physical Security Policy

# Appendix B – Receipt and Acknowledgement

I have read ABC Company’s (Company’s) Facility Security Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name (Printed)