Physical Security Management Policy

Template

This is an example policy. Please ensure you update this policy template so that it is suitable for your organization.

## Objective

The purpose of this policy is to ensure the safety and security of personnel, volunteers, and clients. The aim is to protect our property premises and valuable assets against theft and damage. This policy will help to produce a safe environment to deliver uninterrupted, quality service.

## Summary

This policy provides detailed guidance to ensure staff and management are aware of the procedures to follow concerning physical security within the organization.

The policy will reflect the standards when it comes to physical security measures employed by the organization to ensure the safety and security of personnel, volunteers and clients utilizing our services.

## Introduction

This policy is designed to support employees by raising awareness of security-related policies, processes, and procedures within the organization. This includes issues that may affect the safety and security of staff, volunteers, and clients.

The policy supports a pro-security culture, where the protection of the <organization>’s infrastructure, such as critical, vulnerable, and valuable assets, is the responsibility of all.

## Purpose

As part of <organization>’s commitment to ensure the delivery of a high quality and safe working environment for those who access our facilities (staff, volunteers, and clients), we will:

* recognize and accept obligations relating to the management of security as far as are reasonably practicable.
* ensure the security of people and property within our organization is a concern of all employees, contractors, and volunteers.
* ensure that all possible measures are taken to deliver a secure environment for all who work or receive services.

Accountability for security of the organization lies with the <role>.

Incidents of crime and breaches of security that are particularly sensitive, where employees have been victims of crime and affected, will be provided with support. In addition to this, their wishes around the reporting of criminal offenses will be respected as much as is reasonably possible.

<Organization> believes that effective security is an integral part of all operational activities.

The responsibility for compliance with this policy is delegated to all directors, managers, and staff in line with their position within <organization>. Security is everyone’s business.

## Scope

This policy applies to:

* staff
* authorized third party workers
* volunteers
* clients

## Process requirements

### Physical security

All services provided by the organization must incorporate good security working practices into their operating procedures, together with security design as part of an overall strategy.

The organization will have systems in place to ensure an appropriate response to incidents, which includes:

* recording all physical security incidents – so that trends can be identified and risks assessed.
* Audit Safeguard Reports – indicating trends and the needs for action to be taken in compliance with all relevant security policies through quarterly reports.

### Security of offices

Where suitable all offices must be fully secured when they not in use either during the day or out of hours. It is best practice for offices to:

* Create and maintain, where possible, key management systems. This could be physical key management systems or temporary (interim) procedures.
* Use a risk-based approach to allow only authorized staff – lists of authorized people should be kept with the cabinet keys. These people must complete the key register and sign their entry, should they remove keys from the appropriate storage facility.
* Keep auditable records for cases where an investigation may be required.

### Protection of organization’s property and assets

All valuables or ‘attractive’ items are to be kept in locked containers or rooms when not in use. An asset register will be kept up to date.

Most thieves are opportunists, so taking simple precautions such as this will reduce financial loss to the organization.

It is strongly recommended that computers and similar equipment are logged in and out of a secure room, and recipients are made to sign for the item. This will prevent items from being reported as stolen when they have been rightfully handed to another staff member.

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and <organization>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

Review of this document: annually by <role>.

Next review date: <date month year>.