Security Management Plan

Template

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

# Introduction

We’re committed to maintaining the security and wellbeing of our staff, service users, partners and the surrounding community. Our Security Management Plan is but one aspect of our overall workplace safety efforts. Together, these efforts span personnel, information and asset security and include training and education activities to help ensure our programs’ success.

Responsibility for this program has been vested in by <Organisation> management. Your cooperation with these efforts will help us all maintain a program that accomplishes all of its goals.

We take specific actions toward identifying security-related threats from cyber crime to workplace violence. You (employees) can expand these efforts by reporting concerns and any security breaches immediately.

Your ongoing knowledge and cooperation as well as participation with the Security Management Plans’ efforts will be appreciated, and again, help ensure its success.

Thank you, <NAME> <POSITION>.

Signed by

## Compliance with Applicable Laws, Regulations, and Standards

There are various laws, regulations, and standards that apply to our organisation. We are committed to comply with these.

Details can be found in the following documents Examples Data Protection Policy and Confidentiality Policy

## Information Security Policy

Our organisation has an Information Security Policy that is:

* supported by management
* reinforced by basic information security principles regarding:
  + confidentiality
  + integrity
  + availability
  + regulatory obligations

Details can be found in the following documents: Information Security Policy, Examples Data Protection Policy and Confidentiality Policy

## Management Commitment and Responsibilities

Management commitment and responsibilities include:

* Program management
* Program review and updates
* Development of a review team if hazards are identified, or for deployment after an event to assist in its review
* Assisting with training
* Enforcing disciplinary actions as needed
* Interaction and assistance with regulatory agencies

Details can be found in the following document: Examples Information Security Policy

## Risk Assessment and Analysis

We will perform:

* Frequent Risk and/or Vulnerability Assessments
* Business impact analyses
* Both Personal and Physical Risk Assessments

Security risk assessments will be conducted as we become aware of new or potential threats.

We have complied with Cyber Essentials and gained Cyber Essentials Plus Certification.

OR

We have complied with IASME Governamce and gained IASME Governamce Gold Certification.

The latest penetration test was performed on date. We will maintain our annual Cyber Essentials Plus Certification, and regular penetration tests.

Also see Examples Information Security Policy

## Asset Management and Recording

We have a current list of information security assets (i.e., an Asset Register) including details of who is responsible for them.

Details can be found in our Examples Equipment Log or Asset Register.

Also see Examples Information Security Policy

## Communications

We ensure secure communications by using Antimalware/anti virus e.g. Barracuda Sentinel (Note: be sepecific with which version). This uses the following features (e.g. DMARC "Domain-based Message Authentication, Reporting & Conformance", which ensures email authentication and a reporting protocol. We also use Examples Office 365 which secures emails using TLS (Transport Layer Security). Communications “in transit” are over an encrypted channel from MS cloud, “at rest” and when stored, data is on encrypted Microsoft Cloud servers. Communications are not stored on premises. Phones don’t store data.

Also see Examples Information Security Policy

## Access Control

We have policies that enforce Access Control principles.

Details can be found in the following document: Examples Security Access Control Policy

Also see Information Security Policy

## Information Systems Protection

We have taken steps to protect data in whatever form it may take including being bound to the GDPR and Data Protection guiding principles as evidenced by our CE+ certificate.

Details can be found in the following documents: Examples Data Protection Policy and Working from Home Policy

Also see Information Security Policy

## Preparedness & Recovery

We have Procedures in place to ensure the continuation of services after a critical incident (e.g., including everything from evacuation plans to backing up servers).

Details can be found in the following document Examples Business Continuity Policy

Also see Information Security Policy

## Data Classification

We classify data based on the data's sensitivity (i.e., Data Labels, Data Handling, Data Access levels).

Details can be found in the following document: Examples Information Security Policy

## Incident Response

During an incident we work through and manage an up-to-date contacts list and also a checklist of responsibilities until the incident is over.

We have a post incident requirement to review any 'lessons learnt' that may help to reduce the possibility of such an incident happening again.

Details can be found in the following documents: Examples Personal Data Breach Policy

Also see Information Security Policy

## Human Resources Security Processes

We have HR processes that cover;

* pre-employment checks
* employee screening
* termination of employment

Details can be found in the following documents: Examples Recruitment and Selection Policy

## Training & Awareness

We have a training program that ensured all staff are aware, understand and comply with the policies and procedures covered by this Security Management Plan.

We employ best practices for teaching security training (e.g., create strong passwords, don’t open suspicious emails, give hackers fewer opportunities to hack a system).

Details can be found in the following documents: Examples Data Protection Policy, Training Register, Security Access Control Policy

Also see Information Security Policy

## Supplementary Information

### Proactive Measures in Security Management

We are proactive in preventing security incidents by using such measures as: Examples Barracuda Sentinel and AVAST anti-virus, Cloud 2 Cloud backup, Unifi gateway.

### Teach Best Security Practices

We employ best practices for teaching security training. Specifically, staff are trained in GDPR and Data Privacy, Understanding Phishing Signs, creating strong passwords, recognising suspicious emails and ways to give hackers fewer opportunities to hack the system.

### Intrusion Prevention System (IPS)

We employ technology that helps to detect or prevent unauthorised access to the network. Specifically: Examples Unifi Gateway, Firewall at the perimeter of the office network that is controlled by our IT provider, Barracuda Sentinel and AVAST anti-virus.

### Updates and Patches

All IT equipment automatically downloads all updates to ensure the latest security which is managed by Examples our IT Support Provider.

### Employees’ End User Device Permissions

We have controls in place that prevent the end user from downloading harmful content onto the system. Specifically: Examples All devices have had autorun disabled and local administrative access restricted, and AVAST anti-virus is real time protection managed by our IT Support Provider).

Review of this policy: this will be reviewed annually by the Director.

Next review date: <DATE>