**Southern Airport Maintenance Service**

**Business Security Plan**

**Author : John Smith (DBA IT Works)**

Version: 1.0

Date: 28/05/2023

Status: Draft

**For more information**

|  |  |
| --- | --- |
| Name: Jade Brown  Email: jadebrown@southernairport.com.au |  |

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | **Date** | **Author(s)** | **Change Description** |
| 1.0 | 31/01/2020 | John Smith | *First draft* |
| 1.1 | 25/05/2023 | Andre Alexandrov | Security features |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1. What is a Security Plan? 3](#_Toc94718640)

[2. The process of creating a security plan 3](#_Toc94718641)

[3. How do you evaluate the existing security risks? 3](#_Toc94718642)

[4. Tools to combat security risks 3](#_Toc94718643)

[5. System policies 3](#_Toc94718644)

[6. Procedures 4](#_Toc94718645)

[7. System and data integrity 4](#_Toc94718646)

[a. Control of physical environment 4](#_Toc94718647)

[b. System/network administration 4](#_Toc94718648)

[8. System audits 4](#_Toc94718649)

# What is a Security Plan?

Security plan is a document to identify the vulnerabilities and to make out strategies to keep the business safe and secure. The plan should secure all assets in the business.

# The process of creating a security plan

This business security plan needs inputs from all stakeholders in the company. All stakeholders will need to continuously evaluate the security risks and develop a documented plan that will be tested, implemented and maintained over time. Initially, the plan will be reviewed every 6 months. Risk Assessment involves identifying, evaluating, controlling and mitigating vulnerabilities of potential threats. Revising the plan is an ongoing process. Vulnerability or threat notifications from vendors need to be monitor.

# How do you evaluate the existing security risks?

To evaluate the existing security risk, the management needs to gather a series of information. Very often, on-site assessment needs to be taken to see the issues of security breaches. The risk assessment may look for records of theft, hazards, extortions or corruption. The impacts may affect the financial system, flight schedules, maintenance services, people safety or the company reputation etc. In the evaluation process, need to ask many questions to get the information needed.

# Tools to combat security risks

* Video surveillance – video record of activities on the premises.
* Alarm systems – Alarm systems can be security alarm systems and fire alarm systems in case of emergencies and crimes.
* Access control – Sensitive areas of the business may be controlled with pass cards, keys and pin code etc.
* Staff training – Training the staff can help to reduce the occurrences of crime. Staff need to aware the security threats and how to handle when security breaches has happened.
* IT security – System policies, standards and procedures need to be established to reduce sensitive information being hacked or leaked.

# System policies

* System policies defines the set of procedures that to use the computer systems. Guidelines can be set up for administration of computer resources, control access to data, software installation and maintenance. Actions need to be taken in case of the computer system misuse.
* The polices also overseeing the acquisition, installation, upgrade, repair, relocation and communication services. IT also handles all network/telecom infrastructure of the Southern Airport maintenance services.
* The policies also cover the security in data management. The management has indicated that the data must be accurate and verifiable. The system must ensure the data are stored with confidentiality, availability and integrity. The policies also require to setup processes and procedures that all staff must follow to protect staff or client information.
* The policies cover the communications such as using email, SMS, MMS, instant message and other electronic means to distribute the official messages.

# Procedures

* Securing computers stores sensitive and critical data – Secure the equipment such as servers, desktop computers, or backup tapes depending on the sensitivity and criticality of data being stored. This document offers guideline for classification of the equipment.
* Incident response and investigation – Immediate respond to security breach incidents until it is resolved. Mitigating impacts need to be in place. Detail procedures must include incident reporting, containment, notifications, investigation and recommendation.
* Remove of network access – Must mitigate potential risk from accessing the system by removing the connectivity through the network.
* Access with password – Password must be associated with any database user account. Further guidelines will be established for user to pick strong password.
* Wireless Network Installations – Computers or devices that has wireless access must be approved by the managers to avoid unauthorized access.
* Media disposal – Restricted data may reside on different types of media such as hard disk, USB drive, tape etc. Simple deletion of file does not provide complete protection of sensitive data. Media must be disposed properly through ICT services.
* Users must change their passwords every 90 days
* Users must not use the same password within the same year
* When changing passwords, users must enter in the current password

# System and data integrity

The ICT has the responsibility to ensure the system is performed without unauthorised manipulation, changes. The system can only be accessed by those authorised users.

## Control of physical environment

* Servers are accessible only to system/network administrators.
* Hardware and storage media from hazards such as power surges, heat, dust, magnetism and electrostatic discharge.
* Ensure the transmission media and protect from being tapped.

## System/network administration

* Control system access and maintaining user authorization level.
* Restrict access to sensitive data and maintain the authentication to users.
* Document the system/network administration procedures
* Create backup and recovery plan to deal with occurrence of natural disasters, server failure, virus and power outrages etc.
* Test software update, security controls and recovery procedures.

# System audits

ICT ensures an annual internal security audits are conducted. It verifies the policies and procedures set in the security plan. It ensures that the information system has adequate controls in place to safeguard the assets, maintain data integrity and the operate efficiently to meet the users and organization needs.