Qualitative Risk Assessment Template

All information in this template are examples only\*

## Introduction

## Roles and responsibilities

Subheading

|  |  |
| --- | --- |
| Role | Description and responsibilities |
| CEO | Data Centre Authority responsible for all day-to-day management decisions and for implementing the Data Link’s long and short term plans.  Termination of employee contracts |
|  |  |
|  |  |

## 

## Classification definitions

Subheading

|  |  |
| --- | --- |
| CIA Triad | Requirements |
| Confidentiality | Ensure that assets are viewed only by authorised parties. |
| Integrity |  |
| Availability |  |

|  |  |
| --- | --- |
| Value | Description |
| Confidential | Used for the most sensitive corporate information that must be tightly controlled, even within the organisation. This information must be securely stored and accessed only by authorised personnel.  Highly sensitive data intended for specific use or group of individuals with a legitimate need-to-know. |
| Private/Internal |  |
|  |  |

**Likelihood**

|  |  |
| --- | --- |
| Likelihood | Description |
| Certain |  |
| Highly probable | It is feasible for a threat to exploit the vulnerability. |
| Possible |  |
| Possible but unlikely |  |
| Almost never |  |

**Impact**

|  |  |
| --- | --- |
| Impact | Description |
| Severe | There is economic loss.  There is loss of life.  Legal liabilities and/or breach of SLAs.  There is loss of corporate or public image.  Communications and recovery must be shared with customers. |
| Significant |  |
| Moderate |  |
| Minor |  |
| Minimal |  |

Valuation Criteria

|  |  |
| --- | --- |
| Impact | Description |
| High | It will result in a loss of concern between Data Link and its customers or result in a large legal action or cause Data Link significant revenue or earnings. |
| Medium |  |
| Low |  |

# Information assets and classifications



## People Assets

|  |  |  |  |
| --- | --- | --- | --- |
| **Item ID** | **Asset Category** | **Asset Name** | **Asset Description/Attribute** |
| 001 | Employees | CEO | Role: CEO  Function: Responsible for all day-to-day management decisions and for implementing the Data Link’s long and short term plans.  Security Clearance: X |
|  |  |  |  |

## Procedures Assets

|  |  |  |  |
| --- | --- | --- | --- |
| **Item ID** | **Asset Category** | **Asset Name** | **Asset Description/Attribute** |
| 006 | Procedures | Personal Use of Devices Policy | Policy: Engineers are advised to avoid using their own laptop/device to perform daily tasks.  Intended purpose: To protect Data Link’s assets against virus or malicious software. |
|  |  |  |  |
|  |  |  |  |

## Data Assets

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item ID** | **Asset Category** | **Asset Name** | **Asset Description/Attribute** | **Classification** |
| 011 | Data | Customer account information | Description: Detail information about each current and previous customer (users, services, usage, credentials)  Owner: Data Link  State: Processing | Confidential |
|  |  |  |  |  |

## Software Assets

|  |  |  |  |
| --- | --- | --- | --- |
| **Item ID** | **Asset Category** | **Asset Name** | **Asset Description/Attribute** |
| 021 | Software | Firewall | Description: Network security system that controls incoming and outgoing network traffic based on a set of rules. |
|  |  |  |  |

## Hardware Assets

|  |  |  |  |
| --- | --- | --- | --- |
| **Item ID** | **Asset Category** | **Asset Name** | **Asset Description/Attribute** |
| 031 | Network components | Server | Description: High density heat and dedicated servers.  Quantity: 53  Category: Systems and peripherals  Location: Data Link premises |
|  |  |  |  |
|  |  |  |  |

## Infrastructure Assets

|  |  |  |  |
| --- | --- | --- | --- |
| **Item ID** | **Asset Category** | **Asset Name** | **Asset Description/Attribute** |
| 037 | Infrastructure | Air conditioning systems | Description: System for controlling the humidity, ventilation, and temperature in the building  Category: Protection device  Quantity: X units  Location: Server rooms |
|  |  |  |  |
|  |  |  |  |

## Information Asset Valuation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item ID** | **Asset Name** | **Loss of Confidentiality** | **Loss of Integrity** | **Loss of Availability** |
|  |  |  |  |  |
| 031 | Servers | Medium | Medium | High |
| 032 | Web/application server | Medium | Medium | Medium |

## Information Asset Prioritisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item ID** | **Asset Name** | **Criterion 1: Impact to revenue** | **Criterion 2: Impact to profitability** | **Criterion 3: Impact to public image** | **Weighted score** |
| Criteria weights must total 100 | | 30 | 40 | 30 |  |
| 031 | Servers | 1 | 1 | 1 | 100 |
| 032 | Web/application server | 1 | 1 | 1 | 100 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Threats and Vulnerabilities

Brief definition of threats

## Threats and Vulnerability Assessment

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset IDs** | **Information Asset Type** | **Threat** | **Vulnerability** |
| 031, 037 | Hardware | **Deliberate Threat**  Theft and fraud | * Lax physical security controls. * Disgruntled employee or contractor. * Lax recruiting processes. * External agents have access to the data centre. * Minimum monitoring is done while external agents are present within the premise |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Risk Assessment

The analysis of the system’s vulnerabilities, the threats associated with them, and the probable impact of that vulnerability exploitation results in a risk rating for each missing or partially implemented control. The risk level is determined on the following two factors:

1. Likelihood of Occurrence

It is the probability that a specific vulnerability within Data Link will occur.

1. Impact

It is the consequence of an event, if it occurs.

The risk rating is the point where the likelihood and impact ratings intersect.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Impact | Severe | 15 | 19 | 22 | 24 | 25 | |
| Significant | 10 | 14 | 18 | 21 | 23 | |
| Moderate | 6 | 9 | 13 | 17 | 20 | |
| Minor | 3 | 5 | 8 | 12 | 16 | |
| Minimal | 1 | 2 | 4 | 7 | 11 | |
|  | | Almost never | Possible but unlikely | Possible | Highly probable | Certain | |
| Likelihood | | | | |

The consequence of an event may also result in the loss of availability, integrity or confidentiality of information which could lead to:

* Economic loss
* Additional costs being incurred
* Unable to operate
* Staff injury
* Legal liabilities and/or breach of Service Level Agreements
* Disruption of business operations
* Competitive advantage
* Theft of information
* Identity and financial theft
* Loss of corporate or public image



## Security Risks

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Threat** | **Risk Description** | **Consequence** | **Gross Risk** | | |
| **Impact** | **Likelihood** | **Risk Rating** |
| R03 | Fire/smoke  intentionally or accidentally |  | 1. Economic loss 2. Unable to operate 3. Staff injury 4. Legal liabilities and/or breach of Service Level Agreements | Severe | Possible | 22 |
| R49 | Data breach/disclosure | One customer gains unauthorised access to confidential information of another customer due to failure of controls that provide separation of memory and storage. | 1. Legal liabilities and/or breach of Service Level Agreements | Significant | Possible | 22 |

# Risk Controls

Brief description of the control



## Recommended Controls

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Threat Agent** | **Existing safeguards** | **Recommended Controls** | **Residual Risk** | | | |
| **Impact** | **Likelihood** | | **Risk Rating** |
|  |  |  |  |  |  |  | |
|  |  |  |  |  |  |  | |
| R03 | Fire/Smoke caused intentionally or accidentally | * Protection devices exist (smoke detectors and extinguishers). * Back-up available. | Business Continuity Plan  Human Resources Process  Security Vetting  Additional standard-compliant smoke detectors | Significant | Possible | 18 | |
| R49 |  |  |  |  |  |  | |

# Reference List

Whitman, M.E., Mattord, H.J. (2014). *Principles of Information Security* (5th ed.). United States of America: Cengage Learning