[Company Name & Logo]

**Information Risk Checklist**

**Identifying and managing risks**

**Version: [v1.0]**

|  |  |
| --- | --- |
| Prepared by | |
| Name |  |
| Title |  |

[dd/mm/yyyy]

# Introduction

This check list was created for helping implementers in discovering, distributing, and monitoring important information security risks. The risk is categorized into four primary areas: compliance, confidentiality, integrity, and availability. This helps to make sure that all these areas are properly managed and routinely assessed to keep them in line with ISO 27001 requirements.

1. Confidentiality Risks

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Risk Description** | **Responsible Person** | **Review Date** |
| ☐ | Unauthorized access to sensitive employee data | [Responsible Person] | [dd/mm/yyyy] |
| ☐ | Data leakage from email phishing attacks |  |  |
| ☐ | Insufficient encryption of sensitive data |  |  |
| ☐ | Unauthorized external vendor access |  |  |
| ☐ | Data exposure due to misconfigured cloud storage |  |  |
| ☐ | Insider threat leading to information misuse |  |  |

## 2. Integrity Risks

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Risk Description** | **Responsible Person** | **Review Date** |
| ☐ | Alteration of critical business data | [Responsible Person] | [dd/mm/yyyy] |
| ☐ | Malware affecting the integrity of files |  |  |
| ☐ | Unauthorized modification of system configurations |  |  |
| ☐ | Data corruption from system failures |  |  |
| ☐ | Compromise of file integrity during transfer |  |  |
| ☐ | Insider threat leading to information misuse |  |  |

## Availability Risks

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Risk Description** | **Responsible Person** | **Review Date** |
| ☐ | Data loss due to hardware failure | [Responsible Person] | [dd/mm/yyyy] |
| ☐ | Denial of Service (DoS) attack impacting services |  |  |
| ☐ | Unavailability due to cyber-attacks |  |  |
| ☐ | Power outage disrupting business operations |  |  |
| ☐ | Network failure causing system downtime |  |  |
| ☐ | Application crash affecting service availability |  |  |

## Compliance Risks

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Risk Description** | **Responsible Person** | **Review Date** |
| ☐ | Failure to comply with data protection laws (GDPR) | [Responsible Person] | [dd/mm/yyyy] |
| ☐ | Inadequate vendor management compliance |  |  |
| ☐ | Lack of evidence for audit trails |  |  |
| ☐ | Non-compliance with industry-specific regulations |  |  |
| ☐ | Incomplete documentation for compliance audits |  |  |
| ☐ | Failure to comply with data protection laws |  |  |

* **Risk Description**: A brief explanation of the identified risk.
* **Responsible Person**: Individual or team responsible for managing this risk.
* **Review Date**: The last date this risk was reviewed.