Insert the organization logo by clicking on the image icon

Risk Management Policy Template

Date:

**Document Control**

|  |  |
| --- | --- |
| **Document Title:** | Risk Management Policy Template |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  |
| **Publish Date:** |  |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Objective 4](#_Toc97464686)

[2. Scope 4](#_Toc97464687)

[3. Policy 4](#_Toc97464688)

[4. Risk Appetite 5](#_Toc97464689)

[5. Main Stages of Cyber Risk Management 5](#_Toc97464690)

[5.1 Risk Identification 5](#_Toc97464691)

[5.2 Risk Assessment 5](#_Toc97464692)

[5.3 Risk Treatment 6](#_Toc97464693)

[5.4 Risk Oversight 6](#_Toc97464694)

[6. Other Requirements 7](#_Toc97464695)

[*7.* Policy Enforcement 7](#_Toc97464696)

Objective

The purpose of this policy to determine Cyber security requirements based on best practices and standards for managing cyber security risks in <entity name>, according to considerations of confidentiality, availability and integrity of information and technology assets.

This policy follows national legislative and regulatory requirements and relevant international best practices.

Scope

The scope of this policy covers all <entity name>’s information, software, hardware, databases, applications/programs, network resources are applicable to the <entity name> to conduct its business.

Policy

1. A cybersecurity risk management methodology and procedures for managing cybersecurity risks must be developed, documented, and approved in <agency name>, and it must be aligned with the National Cybersecurity Risk Management Framework. Approved standards and guiding frameworks can be used internationally (eg: ISO27005, ISO31000, and NIST) in developing a cybersecurity risk management methodology.
2. The cybersecurity risk management methodology should cover, at a minimum, the following:
	* Defining the assets and knowing their importance.
	* Identifying and evaluating the risks that affect the business, assets or workers of the <entity name> (for example: the effects of the <entity name> resulting from cyber risks).
	* Identifying and evaluating threats and vulnerabilities related to cyber security that may affect information and technology assets.
	* Determining the methods of dealing with cyber risks.
	* Arranging the cyber risk mitigation measures according to priority and according to specific procedures.
	* Classify and define the levels of cyber risk based on the level of impact and the probability of occurrence of the threat for <entity name>.
	* Create a cybersecurity risk register to document and monitor risks.
	* Define roles and responsibilities for managing and dealing with cybersecurity risks
3. Risk assessment should be carried out periodically to ensure that information and technical assets are protected, and risks are dealt with according to priority.
4. The management of cyber security risks must be compatible with the Enterprise Risk Management “ERM” in <agency name>.

Risk Appetite

1. Risk appetite criteria should be defined and documented, according to the level of risk and the cost of addressing the risk versus its impact.
2. Additional controls must be applied in order to reduce the risk to an acceptable level if the risk appetite is not met.
3. In case the risk acceptance criteria are exceeded, the authorized person will be escalated to take the necessary actions or decisions.

# Main Stages of Cyber Risk Management

1. **Risk Identification**
	1. The <Department of Cybersecurity> must identify events or circumstances that may violate the confidentiality, integrity, and availability of information and technology assets, including in particular the identification of information and technology assets, and the threats that may be exposed and the relevant gaps, and the approved controls, and then determine the effects resulting from the loss of confidentiality, integrity and availability of these assets.
2. **Risk Assessment**
	1. The <Department of Cybersecurity> shall carry out a minimum cybersecurity risk assessment procedure in the following cases:
		* In the early stages of technical projects.
		* Before making a fundamental change in the technical infrastructure.
		* When planning to acquire third party services.
		* When planning and before launching new technical products and services
	2. The risks should be reassessed and updated as follows:
		* periodically for all information and technology assets, and at least annually for sensitive systems.
		* After a cybersecurity incident that violates the integrity, availability and confidentiality of information and technology assets.
		* After obtaining significant audit findings or proactive information.
		* In the event of a change to the information and technical assets.
	3. The risk assessment process should cover the following:
		1. **Risk Analysis:** <The Department of Cybersecurity> should assess the likelihood of threats and their impacts and use the results of this assessment to determine the overall level of these risks. The <Department of Cyber Security> must adopt a quantitative or qualitative methodology for conducting risk analysis.
		2. **Risk Evaluation:** <The Department Concerned with Cyber Security> must estimate the amount of cyber risks in accordance with the institutional risk assessment criteria approved in <entity name>, and determine the methods of dealing with them according to priority
3. **Risk Treatment**
	1. The <Department of Cybersecurity> shall define the risk treatment options according to the following list:
		* **Risk Mitigation:** Addressing or reducing the degree of risk by applying the necessary security controls to reduce the probability of occurrence or impact or both, which help in containing and maintaining risks within acceptable levels.
		* **Risk Avoidance:** Getting rid of the danger by avoiding continuing with the source of the danger.
		* **Risk Transfer:** Sharing risks with a third party that has the capabilities to deal with risks more effectively, or insuring information and technical assets in case they are exposed to cyber risks.
		* **Risk Acceptance:** The level of risk is acceptable, but it must be constantly monitored in case of change.
	2. Risk treatment options should be identified and documented based on the results of the risk assessment, implementation cost and expected benefits.
4. **Risk Oversight**
	1. Risk Monitoring The <Department of Cybersecurity> should prepare and maintain a risk register to document the outputs of the risk management process. It shall include, at a minimum, the following information:
		* The process of identifying risks.
		* Scope of risks.
		* The person responsible or the risk owner.
		* A description of the risks, including their causes and effects.
		* Risk analysis showing the effects resulting from the risks and their time scale.
		* Risk assessment and classification that includes the probability, size and overall classification of risks if they occur.
		* The plan for dealing with risks, including the procedure for dealing with them, the person responsible for them, and their schedule.
		* Description of the remaining risk.
	2. The Key Performance Indicator “KPI” should be used to ensure effective cybersecurity risk management.
	3. The <Department of Cyber ​​Security> shall collect evidence regarding the status of cyber risks and review them periodically.

Other Requirements

* 1. The cybersecurity risk management methodology and procedures should be reviewed and updated at planned intervals (or if changes occur in relevant legislative and regulatory requirements and standards), and changes should be documented and approved.
	2. The cybersecurity risk management policy should be reviewed annually, and changes should be documented and approved.

Policy Enforcement

1. Policy document sponsor and owner: <Head of Cyber Security Department>.
2. Policy implementation and enforcement: <Department Concerned with Information Technology>.
3. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-