INSERT LOGO

PROJECT MANAGEMENT GUIDELINES

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Purpose of This Document

The purpose of this document is to ensure that information security risks related to projects and deliverables are effectively addressed throughout the project management lifecycle.

The document provides comprehensive guidance for integrating information security into project management, ensuring compliance with ISO/IEC 27001:2022 control 5.8.

Security must be built into projects from the ground up, and not added on as an afterthought. Review and follow the guidance in this document, and request support where needed.

Scope

This document applies to all projects managed by [Company Name], regardless of their size, duration, or complexity. It is intended for use by project managers, project team members, and information security personnel.

Roles and Responsibilities

Role	Responsibility
Project Manager	Ensure information security is integrated into all stages of project management.
Risk Manager	Conduct information security risk assessments and manage risk treatment plans.
Security Analyst	Identify and document information security requirements for the project.
Information Security Manager	Develop and maintain security procedures and policies for project activities.

Training Coordinator	Provide training and awareness on information security for project team members.

Procedures

1. Integration into Project Management

Objective	Ensure information security considerations are part of the project management framework.
Actions	• Include reference to information security in project charters and plans. • Address security in all project phases: initiation, planning, execution, monitoring, and closure.
Evidence	• Project management plans, meeting minutes.

2. Risk Assessment and Treatment

Objective	Identify, assess, and treat information security risks.
Actions	• Conduct initial risk assessments during project initiation. • Review and update risk assessments periodically. • Implement risk treatment plans based on assessment outcomes.
Evidence	• Risk assessment reports, risk treatment plans.

3. Define Information Security Requirements

Objective	Establish clear information security requirements for the project.
Actions	• Identify security requirements based on project scope and objectives. • Document requirements in the project documentation.
Evidence	• Requirements documentation, compliance checklists.

4. Monitor and Review Security Measures

Objective	Regularly review and evaluate the effectiveness of security measures.
Actions	• Schedule regular reviews of security measures. • Conduct tests to ensure controls are effective.
Evidence	• Review reports, test results.

5. Allocate Responsibilities

Objective	Clearly define and allocate information security responsibilities within the project team.
Actions	• Assign specific security roles and responsibilities to team members. • Ensure all team members understand their security-related duties.
Evidence	• Responsibility matrix, role descriptions.

6. Document Procedures and Policies

Objective	Maintain comprehensive procedures and policies for integrating security into project activities.
Actions	• Develop and update security procedures and policies as needed. • Ensure procedures are easily accessible to project teams.
Evidence	• Security procedures, policy documents.

7. Training and Awareness

Objective	Provide training and raise awareness on information security for project team members.
Actions	• Conduct regular training sessions on security principles and practices.

	• Disseminate awareness materials related to information security.
Evidence	• Training records, awareness materials.

Appendices

Appendix A: Example Responsibility Matrix

Project Phase	Responsible Role(s)	Security Tasks
Initiation	Project Manager, Risk Manager	Initial risk assessment, security planning
Planning	Security Analyst, Information Security Manager	Define security requirements, develop treatment plans
Execution	Project Manager, All Team Members	Implement security controls, ongoing risk monitoring
Monitoring	Project Manager, Risk Manager	Review and test security measures, update risk assessments
Closure	Project Manager, Information Security Manager	Final security review, document lessons learned

Appendix B: Sample Security Requirements Checklist

Requirement	Description	Status
Access Control	Ensure only authorized personnel have access.	[ ]
Data Encryption	Encrypt sensitive data in transit and at rest.	[ ]
Regular Audits	Conduct regular security audits and reviews.	[ ]
Incident Response Plan	Develop and test an incident response plan.	[ ]
Secure Development Policy	Follow secure coding practices.	[ ]