NetGain systems	No of Pages	**1** of **7**
	Document Classification:	Internal
	Effective Date	1 Aug 2025
INFORMATION SECURITY IN PROJECT MANAGEMENT	Doc No	ISMS-ORG-04
	Revision	1.0

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

This document sets out the organization's guidelines to ensure that information security receives proper consideration throughout the project management process.

It is essential that projects address the issue of how information security will be maintained during the project planning, during the project and once the project has been delivered.

SCOPE

These guidelines apply to projects that cover the whole spectrum of business operations. Internally, it will apply to IT infrastructure enhancements or changes and modifications within the organisation's environment or new systems / applications to be used by the organisation for information hosting/processing. This will also apply to external projects e.g., new projects for clients.

REFERENCE

ISO/IEC 27001 Standard	Annex A 5.8 Information security in project management
	Annex A 5.34 Privacy and protection of PII
	Annex A 8.10 Information deletion
	Annex A 8.11 Data masking
	Annex A 8.12 Data leakage prevention
	Annex A 8.26 Application security requirements

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

The assigned Project Team and where personal data is involved, the DPO shall ensure that the information security and data protection are maintained during the project and after the project is delivered.

PROCEDURE

1 Guidelines

Projects will be managed according to the following stages and documented using the Project Management Plan.

- ***Proposal*** – Project proposal is created and submitted to management for approval.
- ***Planning*** – Approved projects will then be initiated, including the formation of the project team, setting of detailed tasks and timelines.

- ***Design and Execution*** – The deliverables of the project will then be created by the project team in line with the approved project plan. Risks and issues will be managed and progress reports delivered.
- ***Transition*** – Once the project has been verified (for example, through testing where appropriate), and accepted, the project will move into live operation.
- ***Project Closure*** - The project will then be reviewed and formally closed. This happens after a variable period of time defined by the project team.

The information security considerations of each of these stages are described in this document.

2 Project Stages

2.1 Proposal

Any project proposal is likely to contain sensitive information and so must be labelled and protected appropriately in line with the organisation's *Information Classification Policy.*

The contents of the proposal will obviously vary significantly according to the subject area but the following considerations should be included in the proposal where appropriate:

- What information is involved, what are the corresponding information needs and the potential negative business impact which can result from lack of adequate security controls
- The required protection needs of information and other associated assets involved, particularly in terms of confidentiality, integrity, availability
- The level of confidence or assurance required in order to derive the authentication requirements
- Access provisioning and authorization processes, for users as well as for privileged or technical users from relevant project members, to customers and external suppliers
- Informing users of their duties and responsibilities
- Requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements
- Requirements mandated by other information security controls (e.g., interfaces to logging and monitoring or data leakage detection systems)
- Compliance with legal, statutory, regulatory and contractual environment in which the organisation operates
- Level of confidence or assurance required for third parties to meet the organisation's information security policies including relevant security clauses in any agreements or contracts.
- Any additional project costs involved with maintaining or improving information security e.g., hardware, software, people

These aspects must be included at the outset in order to avoid the situation where information security controls have to be retrofitted after the project, with little or no available budget, or the organisation is exposed to an unacceptable level of risk.

2.2 Planning

2.2.1 Roles and Responsibilities

Whilst information security is everyone’s responsibility, there are a number of key roles within a typical project which have specific information security responsibilities. These are:

Role	Responsibilities
Project Team	● Champion and emphasise the importance of good information security and protection of personal data within the project ● Set project objectives ● Identify information security risks ● Determine specific controls ● Ensure that information security controls within the project are maintained effectively ● Assess and investigate information security incidents all throughout the project and report to the management
Data Protection Officer (DPO)	● Be independent and report directly to the appropriate management level of the organization in order to ensure effective management of data protection risks ● Be involved in the management of all issues which relate to the processing of personal data ● Be expert in data protection legislation, regulation and practice ● Act as a contact point for supervisory authorities ● Inform management and employees of the organization of their obligations with respect to the processing of personal data ● Provide advice in respect of data protection impact assessments (DPIA) conducted by the organization

2.2.2 Project Objectives

As part of the planning stage, the project objectives should be set. The objectives will be in line with the following:

- Identification of all relevant information security risks
- Successful implementation of controls to address the risks
- Avoidance of information security breaches

2.2.3 Information Security Risks

Information security risks shall be identified at the start of the project and at several stages of the project, where applicable. Each assessment should consider the assets, personal data involved, and deliverables of the project, their vulnerabilities and the threats that they face during the project. These will include threats to confidentiality, integrity, and availability of information.

2.2.4 Data Protection Impact Assessment (DPIA)

The organisation has adopted the principle of privacy by design and the definition and planning of all new or significantly changed systems that collect or process personal data must be subject to due consideration of data protection issues, including the completion of DPIA.

The DPIA will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing their personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and anonymization should be considered where applicable and appropriate such as the following:

- Not granting all users access to all data, therefore designing masks in order to show only the minimum required data to the user
- Where some data should not be visible to the user for some records out of set of data, designing and implementing a mechanism for partial obfuscation of data
- Encryption (requiring authorized users to have a key)
- Nulling or deleting characters
- Substitution (changing one value for another)
- Replacing values with their hash
- Any legal or regulatory requirement (e.g., requiring the masking of other characters of NRIC if there is no purpose to collect the full NRIC)

For cloud-based products to be acquired, the organisation will rely on cloud-native data loss prevention (DLP) policies, and determine authorisation rules / access rights.

2.2.5 Selection of Controls

Based on the risks that are identified by the DPIA and risk assessment that require treatment, appropriate controls will be selected by the project team. These controls may be in the form of organisational, people, physical, technological controls, or other suitable ways of addressing the risks effectively.

The controls should be documented and all members of the project team made aware of them and the reasons why they have to be / have been put in place.

2.3 Design and Execution

The controls that have been put in place as part of the planning stage should ensure that the information security risks are managed and the project goals are achieved. It may be necessary to update any members of the project team that join after the initial training was delivered. Any third parties involved in the project should also be made aware of the policies and controls that are in place.

Risk management should be a standard item on the agenda of each project meeting and any changes to risks, including the addition of new ones, should be made as soon as they are identified. Any required changes to controls should also be put in place as soon as possible to ensure the continued security of the project's sensitive information including personal data.

Any information security breaches within the project should be notified to the project manager as soon as possible. For data breach, the DPO shall be informed immediately. The project manager and the DPO (in the event of data breach) will then decide what action to take based on the severity, including necessary reporting and escalations.

2.4 Transition

The transition of a project into live running is an event that can be complicated and stressful and it is important that enough thought is given by the project team to how information security will be maintained.

The project must ensure that sufficient verification or testing where appropriate, has been carried out to check that the security controls defined as deliverables of the project work as intended and that adequate training in them has been delivered to the people involved in maintaining them. If the project is to be implemented in phases, the project manager must ensure that adequate controls are in place during each phase and that security is not compromised in the interests of convenience or speed.

Formal internal signoff from the project manager, and for external projects, customer acceptance signoff should be obtained at the end of the verification and/or testing. The project team should also consider whether it would be appropriate to engage a suitable third party for any necessary independent security testing.

2.5 Project Closure

Once the project has been implemented and signed off, a project review meeting will be held to discuss the lessons learned during the project and the achievement of the project objectives. This is an opportunity to raise any information security issues that occurred and to define the best way of preventing them in future projects.

The lessons learned should be documented and any recommended changes incorporated into the project management method in the project closure meeting.

FORMS

ISMS-ORG-04-F1	Project Management Plan