NOVA MERCHANT BANK

INFORMATION SECURITY POLICY

MARCH 2024

Document History

Date	Version	Comment
March 2024	1.0	

Policy	Responsibility			
Owner	**Name:**	**Designation**	**Signature**	**Date**
	Information Security Department.	Chief Information Security Officer		**07/03/2024**
Approval	EXCO:	EXCO Chairman (MD/CEO)		
	Board:	Board Chairman		
Date of next review	07/03/2026			

1 Table of Contents

1.0 Introduction

This policy defines how information security management system will be set up, managed, measured, reported on, and continually improved within Nova Merchant Bank (Nova).

Nova has decided to pursue full certification to ISO 27001:2022 in order that the effective adoption of information security best practice may be validated by an external third party.

The purpose of this document is to define an overall policy regarding the management system that is appropriate to the purpose of Nova and includes:

- A framework for setting objectives
- A commitment to satisfying applicable requirements
- A commitment to continual improvement of the management systems

This policy is available in electronic form and will be communicated within the organization and to all relevant stakeholders and interested third parties.

2.0 Information Security Policies

The organizational context of Nova is set out in the document "***Nova-IMS-0401 Organizational Context and Scope***." Given the fast-moving nature of the business and the markets in which it operates the context will change over time. This document will be reviewed at a minimum, on a biennial basis, or when any significant change occurs. The ISMS will also be updated to cater for the implications of such changes.

3.0 Scope of the ISMS

The boundaries of the Management Systems are defined in the document "***Nova-IMS-0401 Organizational Context and Scope***."

4.0 Commitment to Satisfy Applicable Requirements

A clear definition of the requirements for the management system will be agreed and maintained with top management of Nova so that all activities are focused on the fulfilment of those requirements.

Nova is fully committed to satisfy all applicable requirements related to Information Security and such, all statutory, regulatory, and contractual requirements will also be documented and thus, serve as input to the ISMS planning process.

Specific requirements regarding the security of new or changed systems or services will also be captured as part of the design stage of each project.

It is a fundamental principle of the Nova's ISMS that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings, briefing documents or as determined relevant.

5.0 Top Management Leadership and Commitment

Commitment to the management system extends to senior levels of the organization and will be demonstrated through this ISMS Policy and the provision of appropriate resources to provide and develop the management system and associated controls.

Top management will also ensure that a systematic review of the performance of the management systems is conducted on a regular basis to ensure that objectives are being met and issues are identified through the audit and management review processes. Management review can take several forms including departmental and other management meetings.

6.0 Framework for Setting Objectives and Policy

The high-level objectives for the information security within Nova are defined within the document "***Nova-IMS-0401 Organizational Context and Scope***." These are fundamental to the nature of the business and should not be subject to frequent change.

These overall objectives will be used as guidance in the setting of lower level, more short-term objectives within an annual cycle timed to coincide with organizational budget planning. This will ensure that adequate funding is obtained for the improvement activities identified.

These objectives will be based upon a clear understanding of the overall business requirements, informed by the annual management review with stakeholders.

ISMS objectives will be documented for the relevant financial year, together with details of how they will be achieved. These will be reviewed on an annual basis to ensure that they remain valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001:2022 the control objectives and policy statements detailed in Annex A of the standard will be adopted where appropriate by Nova. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with ***Nova-ISMS-0601 Information Security Risk Assessment and Treatment Plan***. For references to the controls that implement each of the policy statements given please see ***Nova-ISMS-0603 Statement of Applicability.***

7.0 Roles, Responsibilities and Authority

Within the field of Information Security Management, there are several key roles that need to be undertaken to ensure successful protection of the business from risks.

Full details of the responsibilities associated with each of the roles and how they are allocated within Nova are given in a separate document ***Nova-IMS-0502 Roles, Responsibilities and Authorities.***

The ISMS Manager shall have overall authority and responsibility for the implementation and management of the Information Security Management System. Their responsibilities specifically include:

- The identification, documentation, and fulfilment of applicable requirements.
- Implementation, management, and improvement of risk management processes.
- Integration of processes.
- Compliance with statutory, regulatory, and contractual requirements in the management of assets used to deliver products and services.
- Reporting to top management on performance and improvement

8.0 Continual Improvement Policy

Nova policy regarding Continual Improvement is to:

- Continually improve the effectiveness of the ISMS across all areas within scope.
- Enhance current processes to bring them in line with good practices as defined within the ISO/IEC 27001:2022 standards.
- Achieve certification to the management system and maintain them on an on-going basis.
- Increase the level of proactivity (and the stakeholder perception of proactivity) about the ongoing management of the ISMS.
- Make processes and controls more measurable in order to provide a sound basis for informed decisions.
- Achieve an enhanced understanding of and relationship with the business units to which the ISMS applies.
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data.
- Obtain ideas for improvement via regular meetings with stakeholders and document them in a Continual Improvement Log.
- Review the Continual Improvement Log at regular management meetings in order to prioritize and assess timescales and benefits.

Ideas for improvements may be obtained from any source including employees, customers, suppliers, risk assessments and service reports. Once identified they will be added to the ***Nova-IMS-1003 Continual Improvement Log*** and evaluated by the ISMS Manager.

If accepted, the improvement proposal will be prioritized in order to allow more effective planning.

9.0 Approach to Managing Risks

A risk management strategy and process will be used which is line with the requirements and recommendations of the management system. This requires that relevant assets are identified, and the following aspects considered:

- Threats
- Vulnerabilities
- Impact and likelihood before risk treatment
- Risk Treatment (e.g., reduction, removal, transfer)
- Impact and Likelihood after risk treatment
- Function responsible/Owner
- Timescale and Review Frequency

Risk management will take place at several levels within the ISMS, including:

- Management planning – risks to the achievement of objectives
- Information security and business continuity risk assessments
- Assessment of the risk of changes via the change management process
- At the project level as part of the management of significant business change

High level risk assessments will be reviewed on an annual basis or upon significant change to the business or service provision. For more detail on the approach to risk assessment please review the documents ***"Nova-ISMS-0603 Information Security Risk Assessment and Treatment Process".***

10.0 Human Resources

Nova will ensure that all staff involved in the ISMS are competent based on appropriate education, training, skills, and experience.

The skills required will be determined and reviewed on a regular basis together with an assessment of existing skill levels within Nova Training needs will be identified, and a plan maintained to ensure that the necessary competencies are in place.

Training, education, and other relevant records will be kept by the Human Resources Department to document individual skill levels attained.

11.0 Auditing and Review

Once in place, it is vital that regular reviews take place of how well the ISMS processes and procedures are being adhered to. This will happen at three levels:

- Structured regular management review of conformity to policies and procedures.
- Internal audit reviews against the management system standards by the Nova Audit Team.
- External audit against the standards in order to gain and maintain certification.

Details of how internal audits will be carried out can be found in ***Nova-IMS-0903 Internal Audit Procedure.***

12.0 Documentation Structure and Policy

All policies and plans that form part of the ISMS must be documented. This section sets out the main documents that must be maintained in each area.

Details of documentation conventions and standards are given in the ***Nova-IMS-0705 Procedure for the Control of Documents and Records.***

Several core documents will be created and will be maintained as part of the ISMS. They are uniquely numbered, and the current versions are tracked in ***Nova-IMS-0703 Documentation Log.***

13.0 Control of Records

Keeping of records is a fundamental part of the ISMS. Records are key information resources and represent evidence that processes are being carried out effectively.

The controls in place to manage records are defined in the document ***Nova-IMS-0705 Procedure for the Control of Documents and Records.***

14.0 Disciplinary Action for Non-Compliance

Users must understand and agree to comply with the IMS Policy and Objectives.

Non-compliance may result in Disciplinary action.

15.0 Policy Review

This policy shall be reviewed once every two years or whenever there is a revised legislation that will necessitate an earlier review.