External Information Security Policy

Version 1.0 – March 2025

Purpose

Nobly's Information Security Policy (hereafter "Policy") establishes our security framework, guiding compliance with legal requirements and best practices. Security is both a necessity and a quality standard for delivering trusted services to clients, partners, and stakeholders.

This Policy ensures the protection of all resources involved in data processing and communication, covering both technological and organizational aspects. It aligns with our Data Protection Policy to support a risk-based security approach.

Objectives

Nobly's security objectives are:

- That our information risks are identified, managed and treated according to an agreed risk tolerance
- That our authorized users can securely access and share information in order to perform their roles
- That our procedural and technical controls balance user experience and security
- That our contractual and legal obligations relating to information security are met
- That individuals that access our information, are aware of their information security responsibilities
- That incidents affecting our information assets are resolved and learnt from, to improve our security

Scope

This Policy applies to the following:

- All employees of Nobly, regardless of employment, including external consultants and service employees. It is expected that the Policy will be complied with.
- All systems, assets, and data in Nobly's possession. Security expectations for third-party vendors and partners are outlined in contractual agreements and risk management frameworks.
- Suppliers and business partners who have access to the organisation's systems and data must also have knowledge of and follow the Policy.

Furthermore, the Policy constitutes a clarification of Nobly's information security strategy and covers all technical and administrative matters that directly or indirectly have influence on operations and use of Nobly's IT systems and data storage.

Policy statement

It is Nobly's policy to ensure that information is protected from a loss of:

- Confidentiality: Information shall be accessible only to authorised individuals
- Integrity: The accuracy and completeness of information shall be maintained
- Availability: Information shall be accessible to authorised users and processes when required

Nobly has implemented an Information Security Management System (ISMS) based on certified standards as required. Nobly is mindful of the approaches adopted by our stakeholders and has adopted a risk-based approach to the application of the following controls:

Policy for information security

Information security must support Nobly's business in relation to:

- Ensuring stability in the approach to data
- Confidentiality in relation to sensitive data
- Reliability in data content

This is ensured by our day-to-day business complying with generally recognised standards for information security. This way, information security ensures that Nobly will continue to be able to live up to the stakeholders and customers' expectations of credibility.

A set of controls, processes and procedures for information security are defined, in support of this policy and its stated objectives.

Organisation of information security

Nobly has established governance arrangements to ensure the effective management of information security, which includes:

- Defined roles and responsibilities: Security responsibilities are clearly assigned to ensure proper oversight and implementation of security measures.
- Management commitment: Leadership supports and enforces security policies to align with business objectives.
- Security implementation and control: Security processes are actively initiated, managed, and monitored to maintain a secure operational environment.
- Ongoing review: Security governance is regularly reviewed and improved to address emerging risks and business changes.

Human resources security

Nobly's security policies and expectations for acceptable use are communicated to all personnel to ensure that everyone understands their responsibilities. In order to further secure this understanding, education and training in information security are available and mandatory for all staff.

Poor or inappropriate behaviour will be addressed, in order to maintain a high level of security.

Where practical, security responsibilities are included in role descriptions, personnel specifications and personal development plans.

Asset management

All assets are documented and accounted for.

Owners are identified for all assets and are responsible for the maintenance and protection of their assets.

All information assets are classified according to their legal requirements, business value, criticality and sensitivity. Classification indicates appropriate handling requirements. All information assets have a defined retention and disposal schedule.

Access control

To protect sensitive information and systems, Nobly has an access control policy which ensures that only authorised person-

nel have access to specific resources, minimizing the risk of data breaches and unauthorised activities.

All users, applications, and systems are granted only the minimum level of access required to perform their duties. Access rights are regularly reviewed and adjusted based on role changes, project requirements, or employment status updates.

All systems require strong, multi-factor authentication (MFA) where applicable, and passwords must meet complexity requirements.

Cryptography

Nobly employs cryptographic techniques to protect sensitive information and ensure secure communication. Encryption is applied to safeguard data in transit and at rest, in line with industry best practices and regulatory requirements.

We adhere to internationally recognized standards for cryptographic controls, ensuring:

- Data confidentiality: Encryption mechanisms prevent unauthorized access to sensitive information.
- Data integrity: Cryptographic hashing and digital signatures help verify data authenticity and prevent tampering.
- Secure transmission: Encrypted channels are used for data exchanges to mitigate interception risks.

Nobly continuously evaluates and updates cryptographic practices to align with evolving security threats and compliance standards, which is outlined in our internal policy for the use of cryptography.

Operations security

Nobly enforces strict operational security measures to protect sensitive information and maintain integrity. These measures help prevent unauthorized access, data leaks, and other security risks.

To ensure a secure operational environment, Nobly implements:

- Access controls: Authentication mechanisms limit system access to authorised personnel only, based on least privilege.
- System monitoring: Continuous monitoring and logging of system activity help detect and respond to anomalies, unauthorised access, or potential threats.
- Patch management: Regular updates and security patches are applied to protect against vulnerabilities and emerging threats.
- Malware protection: Advanced threat detection and antivirus solutions help prevent, detect, and mitigate malicious activity.
- Change management: Secure processes govern system updates, ensuring modifications are reviewed, tested, and approved before implementation.
- Incident response: A structured response framework allows for quick identification, containment, and resolution of security incidents to minimize impact.
- Backup and recovery: Secure backup procedures and disaster recovery plans ensure business continuity in case of system failures or cyber incidents.

Nobly continuously enhances its operational security practices to align with industry standards, regulatory requirements, and evolving threat landscapes.

Communications security

Nobly will maintain network security controls to ensure the protection of information within its networks. Nobly also provides guidance to ensure the secure transfer of information both within its networks and with external entities. This is in line with the classification and handling requirements associated with that information.

System acquisition, development and maintenance

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Controls to reduce any risks identified will be implemented where appropriate.

Systems development will be subject to change control and separation of test, development and operational environments.

Supplier relationships

Our company relies on third-party suppliers and service providers for various business functions, including cloud infrastructure, software components, and professional services. While these suppliers do not have direct access to our internal assets, their security posture can impact our overall risk profile.

Therefore, suppliers are expected to comply with:

- GDPR
- Applicable national and international regulations on data protection
- Human rights
- Labour practices
- Other relevant industry standards and legislation

Risk & incident management framework

An annual risk assessment is performed based on Nobly's risk management policy and methodology, which is based on ISO 31000. An overview of the current threat landscape is outlined, and individual assessments are made on all systems and suppliers.

Identified risks that might threat Nobly's operations are logged in the risk assessment & business impact matrix. Based on likelihood and probability, each risk is ranked, linked up with, and described further in either the Disaster recovery plan, the Business continuity plan or both.

All incidents are treated based on Nobly's incident response plan and logged in the compliance tool for future reference.

Information security aspects of business continuity management

In order to protect critical business processes from the effects of major failures of information systems or disasters, Nobly has a disaster recovery plan in place. This is to ensure timely recovery in line with documented business needs. This includes appropriate backup routines and built-in resilience.

Business continuity plans are maintained and tested in support of this policy, as well as an annual business impact analysis, detailing the consequences of e.g.:

- Disasters
- Security failures
- Loss of service/service availability
- Hardware/software failure
- Human error
- Supply chain disruptions
- Regulatory non-compliance
- Power outages
- Pandemics or health crisis
- Loss of critical personnel

Compliance monitoring

The design, operation, use and management of information systems must comply with all laws, regulations and contractual security requirements.

Nobly uses a combination of internal and external audits to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures. This includes penetration tests, IT health checks, gap analyses against documented standards and internal checks on staff compliance and an annual ISAE 3000 type 2 declaration.

Review

A review of this policy will be undertaken by the information security forum and management annually or more frequently as required and will be approved by the CEO.