Information Security Policy

Comprehensive Security Strategies

NODA Intelligent Systems AB

2023-11-28

NODA

Contents

1 Legal Disclaimer and Copyright Notice

1.1 Disclaimer

This Information Policy represents the official information security policies and procedures of NODA Intelligent Systems AB as of the publication date. While we strive to keep our policies current with the latest security standards and practices, technological changes and threats may necessitate updates without prior notice. This document is intended to inform and guide our partners and stakeholders about our information security posture and expectations.

NODA Intelligent Systems AB is not liable for any consequences arising from the application or misinterpretation of the policies in this document. Partners and stakeholders should use this document in conjunction with their security policies and alignment with applicable laws and regulations.

1.2 Copyright and Trademark

1.3 Contact Information

For additional information or assistance, please contact:

NODA Intelligent Systems AB Headquarters
Address: Biblioteksgatan 4, 374 35 Karlshamn, SWEDEN
Phone: +46 454 10 271
Email: info@noda.se

NODA Intelligent Systems AB Technical Support
Phone: +46 454 10 271
E-mail: support@noda.se
Online: https://www.noda.se

2 Changelog

The changelog section documents all notable changes to the Information Security Policy document. It is crucial for tracking the evolution of the policy and ensuring transparency in how security procedures are updated over time.

2.1 [1.0.0] - 2023-TBD

- Initial version of the Information Security Policy document.

2.1.1 Sections Included

- Introduction
- Executive Summary
- Governance
- Risk Management
- Asset Management
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance
- Policy Adoption
- Appendices (A-E)

Note: Versions are denoted using Semantic Versioning (MAJOR.MINOR.PATCH). Major updates involve substantial changes or additions, minor updates involve small changes or additions, and patches are typically for minor corrections or clarifications.

3 Introduction

3.1 Purpose

The purpose of this Information Security Policy ("Policy") is to protect NODA Intelligent System's (NODA) information assets from all threats, whether internal or external, deliberate or accidental. This policy establishes a framework for maintaining confidentiality, integrity, and availability of company information and managing related security risks.

The objective is to ensure business continuity, minimise damage, and maximise return on investments and business opportunities. This policy also ensures that the company complies with all applicable laws, regulations, and standards concerning information security, including the GDPR and the NIS 2 directive.

3.2 Scope

This policy applies to all employees, contractors, suppliers, and other parties with access to information systems and data owned or managed by NODA. It covers all forms of technology and media, including (but not limited to) computer equipment, software, operating systems, storage devices, network devices, e-mail, data, and any form of electronic communication.

The scope of this policy also extends to all forms of information processing, encompassing the entire lifecycle of information at NODA, including creation, processing, storage, transmission, and destruction.

3.3 Information Security Objectives

NODA's information security objectives are to:

- Protect the confidentiality of company data to prevent unauthorised disclosure.
- Maintain the integrity of company data to ensure its accuracy and completeness.
- Ensure company data and IT services are available for authorised users when required.
- Comply with legal and regulatory requirements concerning data protection and privacy.
- Educate and train all stakeholders on their roles and responsibilities concerning information security.
- Establish controls and procedures for responding to and managing security incidents.

3.4 Compliance Obligations

NODA is committed to complying with all relevant compliance obligations including, but not limited to:

- General Data Protection Regulation (GDPR): Ensuring all personal data of EU citizens are processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage.
- Swedish Law.

This policy will be reviewed and updated regularly to comply with any changes in the law, organisational policies, or contractual obligations. It will also consider changes in the threat landscape and advancements in technology.

4 Executive Summary

The Information Security Policy Document of NODA encapsulates our comprehensive approach to safeguarding our information assets against various threats. This document guides all employees, contractors, and associated parties, ensuring everyone is aligned with our security principles and practices.

Key Highlights:

- **Governance**: Outlines the structure and responsibilities within our organisation for overseeing and implementing information security measures.
- **Risk Management**: Details our strategies for identifying, assessing, and mitigating IT risks, tailored to our unique operational needs.
- **Asset Management**: Describes the processes for managing the lifecycle of our information assets, from identification to disposal, ensuring their security and integrity.
- **Human Resources Security**: Focuses on the critical role of our people in maintaining security, covering aspects from pre-employment screening to post-employment obligations.
- **Physical and Environmental Security**: Addresses the security of our physical spaces and hardware, particularly considering our operations in a rented office space.
- **Communications and Operations Management**: Details the procedures for managing our IT systems and communications, emphasising operational integrity and data protection.
- **Access Control**: Describes how access to our systems and data is controlled and monitored to prevent unauthorised access and ensure data confidentiality.
- **Information Systems Acquisition, Development, and Maintenance**: Ensures that security is integral to our systems throughout their lifecycle.
- **Information Security Incident Management**: Outlines our approach to effectively managing and responding to security incidents.
- **Business Continuity Management**: Describes our strategies for maintaining business operations in the face of disruptions, focusing on information security.
- **Compliance**: Emphasises our commitment to adhering to legal, regulatory, and contractual requirements in all aspects of our IT operations.
- **Policy Adoption**: Discusses the process of policy approval, dissemination, and enforcement within our organisation.

This document aligns with the latest legal and regulatory requirements and reflects our commitment to best practices in information security. By adhering to the policies and procedures outlined herein, NODA aims to protect its critical information assets, ensuring business resilience and the trust of our clients and partners.

5 Governance

Information security governance within NODA is structured to ensure clear accountability and efficient information security management aligned with business objectives and compliance requirements.

5.1 Information Security Organisation

The Information Security Organization within NODA comprises individuals and teams responsible for implementing, monitoring, and enforcing security policies and procedures. It is headed by the chief technology officer (CTO), acting as the chief information security officer and reporting directly to the CEO.

5.1.1 Chief Information Security Officer (CISO)

- Responsible for the overall direction of information security functions.
- Develops and maintains the Information Security Policy.
- Coordinates with department heads to align security with business activities.

5.1.2 Information Security Team

- Implements security measures and manages day-to-day security operations.
- Monitors systems for security incidents and responds accordingly.
- Provides training and support to staff on information security matters.
- Establishes information security requirements for procuring third-party products and services, ensuring they meet the organisation's security standards.

5.2 Roles and Responsibilities

Each individual in the company, from executive management to the operational staff, has a role in securing the company's information assets. Clear roles and responsibilities are defined and communicated as follows:

5.2.1 Management Responsibilities

- Approve and provide resources for the information security program.
- Promote a culture of security awareness throughout the organisation.

5.2.2 Employee Responsibilities

- Adhere to the Information Security Policy in their day-to-day work.
- Report any observed security incidents or weaknesses.
- Participate in Information Security training.

5.2.3 Technology Department Responsibilities

- Implement and maintain technical security solutions.
- Ensure backup and recovery processes are effective and tested regularly.

5.2.4 Third Parties

- Comply with the Information Security Policy and any additional security requirements that apply to their scope of services.
- Participate in regular security reviews and audits as required.

5.3 Policy Review and Update Process

The Information Security Policy shall be reviewed annually or as required by changes in the legal, technical, operational, or business environment. The review process includes:

5.3.1 Annual Review

- Evaluate the effectiveness of existing security policies.
- Incorporate feedback from staff, management, and external stakeholders.

5.3.2 Update Mechanism

- Document changes and communicate updates to all stakeholders.
- Ensure that revisions are made in a controlled manner with proper approval.

5.3.3 Documentation

- Maintain historical versions of the policy for audit and compliance purposes.
- Keep a record of changes to understand the evolution of the security strategy.

The governance model for information security is fundamental to ensuring that the policy remains practical and relevant. All staff members are required to be familiar with the policy, and it is the responsibility of management to enforce compliance.

6 Risk Management

At NODA, recognising the unique challenges and dynamics of a small business environment, we adopt a tailored approach to risk management. This section provides a simplified yet robust framework for identifying, assessing, and addressing IT risks. We aim to ensure that risk management processes are feasible and effective, aligning with our operational scale and resource availability.

6.1 Risk Assessment Process

6.1.1 Team-Based Risk Identification

- Regularly, in team meetings, discuss potential risks in a brief, focused manner. Use this time to identify any new threats or changes in our operational environment.
- Keep a simple, shared document to list identified risks and notes from these discussions.

6.1.2 Practical Risk Classification

- Classify risks informally into 'Immediate Attention', 'Monitor', and 'Low Priority' categories. Focus on what's actionable and relevant to our current operations.

6.2 Risk Treatment

6.2.1 Action-Oriented Response Planning

- Quickly decide on practical steps to mitigate high-priority risks. Solutions might include basic procedure adjustments, quick-fix security enhancements, or short training sessions.
- Assign simple action items from these meetings to team members, ensuring clear accountability.

6.3 Ongoing Risk Monitoring

6.3.1 Informal Continuous Monitoring

- Foster a culture of awareness where all team members are encouraged to watch and promptly communicate any potential risks or irregularities.
- Integrate risk monitoring into regular work routines, avoiding the need for extensive separate processes.

6.3.2 Bi-Annual Review

- Set aside time twice a year to formally review our risk landscape. It can be part of a regular team meeting and doesn't need to be a lengthy process.
- Update our shared risk document accordingly and adjust our risk treatment plans as necessary.

In our business environment, risk management is about being proactive yet practical. We focus on the most significant risks to our operations, ensuring that our approach is manageable and effective without imposing excessive administrative burdens.

7 Asset Management

Asset management aims to ensure that NODA's information assets are appropriately identified, classified, and managed throughout their lifecycle to protect them from unauthorised access, alteration, disclosure, or destruction.

7.1 Inventory of Assets

7.1.1 Asset Inventory Maintenance

- Maintain an inventory of all information assets, including hardware, software, documentation, and data.
- Ensure the inventory is kept current and reflects any additions, changes, or disposals of assets.

7.1.2 Asset Ownership

- Assign a designated owner to each asset who is responsible for the asset's maintenance and protection.
- The asset owner should be knowledgeable about the asset and capable of managing the associated risks.

7.2 Ownership and Classification

7.2.1 Asset Classification

- Classify assets based on their sensitivity and criticality to NODA's business operations.
- Categories should include, at a minimum, Confidential, Internal, and Public classifications.

7.2.2 Classification Criteria

- Develop straightforward criteria for categorising our information assets. These criteria will consider the nature of our business, the sensitivity of the data, and any legal or regulatory requirements we must meet.
- Conduct brief, targeted training sessions to ensure that all team members understand how to handle different types of information based on these categories. This training will focus on the practical aspects of data handling relevant to our daily operations.

7.2.3 Periodic Review and Reclassification

- Conduct regular reviews of asset classifications to ensure they remain appropriate as the business and external environment evolve.

7.3 Handling Requirements

7.3.1 Handling Procedures

- Implement straightforward procedures for managing the lifecycle of information assets aligned with their classification. This includes guidelines for handling, storing, transmitting, and securely disposing of assets.
- Tailor these guidelines to be easily integrated into daily operations, ensuring they are clear and concise for IT professionals.

7.3.2 Access Restrictions

- Apply the principle of least privilege to limit access to sensitive assets. Ensure team members can only access the information necessary for their job functions.
- Given the technical proficiency of our staff, utilise efficient access control mechanisms, possibly leveraging existing IT tools or systems for monitoring and managing access.

7.3.3 Data Loss Prevention

- Utilise Data Loss Prevention (DLP) strategies appropriate for a small, skilled IT team. It may include configuring network and endpoint solutions to monitor and protect sensitive data.
- Focus on practical encryption practices for safeguarding data at rest and in transit, using industry-standard encryption tools and protocols.

7.3.4 Transfer and Removal of Assets

- Establish clear procedures for the secure internal transfer and external movement of assets. Ensure these straightforward processes reflect the frequency and nature of such transfers in our business.
- When assets are taken off-premises or transferred electronically, apply suitable security measures based on the asset classification and existing IT infrastructure capabilities.

7.3.5 Disposal and Destruction

- Implement policies for the secure disposal or destruction of assets, ensuring that no sensitive data can be recovered from discarded assets.
- For electronic assets, follow data wiping or destruction standards that meet Swedish and EU regulatory requirements.

By effectively managing its assets, NODA can ensure the security and integrity of its information and IT infrastructure. Asset management should be a collaborative effort involving all departments within the company to achieve comprehensive protection.

8 Human Resources Security

Our people play a pivotal role in the information security landscape at NODA. This section delineates policies to foster a culture of security awareness and responsibility among our team members.

It encompasses the entire journey of an employee with NODA, starting from the recruitment process and extending beyond their tenure with us. Our goal is to instil a deep understanding of each individual's impact on our information security at every stage of their association with the company.

8.1 Pre-employment

8.1.1 Candidate Evaluation

- Implement a streamlined, legally compliant background check process for prospective employees, emphasising aspects pertinent to their role and organisational fit. This process, in alignment with Swedish privacy laws, includes thorough reference verification and professional history review to ensure alignment with our company values and operational requirements.
- Incorporate confidentiality and data protection commitments into employment contracts, ensuring alignment with GDPR and other pertinent legislation.

8.1.2 Security Awareness in Employment Terms

- Articulate information security responsibilities in employment agreements.
- Outline expectations around information security and consequences of policy violations to ensure clarity from the onset.

8.2 Employee Engagement

8.2.1 Awareness, Education, and Training

- Engage employees in regular, interactive training sessions tailored to their specific roles, focusing on information security and privacy best practices.
- Maintain a dynamic security awareness program that includes regular updates on emerging threats and policy changes.

8.2.2 Job Responsibility

- Clearly define and communicate the security responsibilities associated with each role, particularly for positions that handle sensitive data.
- Ensure employees designated with specific security duties have the expertise and support to perform their roles effectively.

8.3 Employment Transition

8.3.1 Offboarding Protocol

- Follow a structured offboarding process to retrieve company assets and revoke system access upon an employee's departure.
- Conduct exit interviews emphasising ongoing confidentiality obligations.

8.3.2 Role Changes

- Reassess and modify access privileges when employees change roles, ensuring they align with new responsibilities.
- Provide additional vetting or training for employees moving into roles with increased data sensitivity.

8.4 Post-Employment

8.4.1 Maintaining confidentiality

- Reinforce the understanding that confidentiality agreements extend beyond the term of employment.

NODA recognises that a proactive approach to human resources security can prevent many security incidents. This policy lays the foundation for a secure, vigilant workforce that protects and respects the company's information assets.

9 Physical and Environmental Security

For NODA, operating in a rented office space, physical and environmental security measures are adapted to our context. This section outlines our approach to ensuring the safety and security of our physical assets and data in a rental environment.

9.1 Secure Areas

9.1.1 Physical Access Controls

- Implement practical access control measures that align with our rental agreement. Depending on the facility's provisions, this may include keycard access systems or traditional lock-and-key mechanisms.
- Maintain a log of issued keys or access cards and ensure their return or deactivation when an employee leaves the company.

9.1.2 Visitor Management

- Accompany visitors at all times within secure or sensitive office areas.

9.2 Equipment Security

9.2.1 Equipment Placement and Protection

- Position critical equipment such as servers (if any) in less accessible areas and secure them appropriately.
- Ensure portable devices like laptops are stored securely when not in use, especially overnight or when the office is unattended.

9.2.2 Power Supply Security

- Utilise surge protectors and uninterrupted power supplies (UPS) to safeguard against power fluctuations and outages.

9.2.3 Cabling Security

- Organise and secure cables to prevent accidental unplugging, tripping hazards, or potential tampering.
- Use cable management solutions to keep cables organised and out of sight.

9.2.4 Equipment Maintenance

- Schedule regular maintenance for all IT equipment, documenting any repairs or updates.

9.2.5 Asset Disposal

- Follow secure disposal procedures for electronic equipment, ensuring that all data is completely erased or destroyed before disposal.

9.3 General Controls

9.3.1 Access Control Policies

- Regularly review who has access to the rented space and make adjustments as necessary, particularly in response to personnel changes.

9.3.2 Clear Desk and Clear Screen Policy

- Enforce a clear desk policy where employees are encouraged to secure sensitive documents and devices when not in use.
- Implement an automatic screen lock policy for all computers to activate after a period of inactivity.

While our status as tenants influences some aspects of physical and environmental security, NODA remains committed to protecting our physical assets and information within the constraints and opportunities of our rented space. We actively collaborate with property management to enhance security measures and ensure a safe working environment.

10 Communications and Operations Management

Efficient management of communications and operations is vital for the integrity and protection of NODA's data and IT infrastructure. This section presents streamlined policies and procedures to oversee our technological resources and safeguard information assets.

10.1 Operational Procedures and Responsibilities

10.1.1 Operating Procedures

- Keep a concise record of procedures for all IT systems and operations, ensuring they are easily accessible and user-friendly.
- Regularly revise these documents to keep pace with operational changes or technological advancements.

10.1.2 Change Management

- Adopt a flexible change management approach that ensures all modifications to IT systems are well-documented and undergo a security review.

10.2 Management of Third-Party Services

10.2.1 Service Agreement Oversight

- Secure agreements with third parties that specify clear security obligations.
- Periodically evaluate third-party security performance to maintain compliance.

10.2.2 Review and Audit

- Consistently monitor third-party services for adherence to agreed standards.
- Conduct periodic audits to assess and ensure compliance with our security expectations.

10.3 System Planning and Acceptance

10.3.1 Efficient Capacity Management

- Continuously monitor and assess system usage, planning for future needs while prioritising security.
- Balance capacity planning with security considerations to meet current and future business demands.

10.3.2 System Acceptance Testing

- Rigorously test new systems, upgrades, and versions before deployment.
- Verify that all new systems comply with our established security standards.

10.4 Malware Protection

10.4.1 Malware Defense Strategies

- Implement and maintain effective malware protection solutions across relevant systems.

10.4.2 User Malware Awareness

- Educate team members about malware risks and emphasise their role in preventing security breaches.

10.5 Data Backup

10.5.1 Robust Backup Strategy

- Develop and execute a strong backup policy, ensuring consistent backups of critical business data.
- Securely store backups offsite to safeguard against local disasters.

10.5.2 Backup Validation

- Frequently test backup systems to guarantee reliability and quick data recovery when necessary.

10.6 Network Security

10.6.1 Implementing Network Safeguards

- Deploy network security measures to protect data and connected services.
- Conduct regular reviews and tests of these security controls.

10.6.2 Network Segmentation

- Use network segregation strategies to enhance security and limit unauthorised access.

10.7 Handling of Media

10.7.1 Secure Media Disposal

- Ensure the secure destruction of any media containing sensitive or confidential data.

10.8 Secure Information Exchange

10.8.1 Transfer Protocols

- Set up secure procedures for transferring information within and outside the organisation.
- Encrypt sensitive data in transit to prevent unauthorised access.

10.9 Proactive System Monitoring

10.9.1 Active System Surveillance

- Utilise monitoring tools to detect unauthorised activities and potential security incidents.
- Regularly inspect system logs for any unusual or suspicious patterns.

10.9.2 Audit Trail Maintenance

- Keep detailed audit logs to support security investigations and monitor access controls.

11 Access Control

Ensuring robust access control is vital for safeguarding NODA's information assets against unauthorised access while facilitating rightful user access to necessary information and resources. This section outlines the established policies and procedures designed to manage and regulate access to our systems and data effectively.

11.1 Access Control Policy

11.1.1 Access Control Standards

- Implement access control standards based on least privilege and need-to-know principles.
- Ensure that access rights are granted according to an approved authorisation process.

11.1.2 Review and Removal of Access Rights

- Regularly review user access rights and remove or adjust them as necessary, particularly when users change roles or leave the company.

11.2 User Access Management

11.2.1 Registration and Deregistration

- Establish a formal user registration and deregistration process to enable, modify, or restrict user access.
- Ensure timely updates of access rights following any changes in user employment status or responsibilities.

11.2.2 User Access Provisioning

- Assign access rights based on job role and function.
- Require authorisation from management for access to restricted systems and data.

11.3 User Responsibilities

11.3.1 Password Management

- Users must follow good security practices in creating and managing their passwords.
- Implement mandatory password complexity and change frequency requirements.

11.3.2 Unattended User Equipment

- Users must apply secure screen locks when systems are unattended.
- Implement automatic screen locking mechanisms after a predefined period of inactivity.

11.4 Network Access Control

11.4.1 Network Access Restrictions

- Control access to network services based on business and security requirements.
- Utilise firewalls and other network segmentation methods to restrict access.

11.4.2 Remote Access

- Implement secure methods for remote access, such as VPNs with strong authentication.
- Regularly monitor and review remote access activities.

11.5 Operating System Access Control

11.5.1 Secure Log-on Procedures

- Enforce controlled access to operating systems with secure log-on procedures.
- Use multi-factor authentication for access to sensitive systems.

11.5.2 User Privilege Management

- Regularly review and adjust user privileges to align with current job requirements.

11.6 Application and Information Access Control

11.6.1 Information Access Restriction

- Implement application-level access controls to restrict access to information and application system functions in line with the access control policy.

11.6.2 Sensitive System Isolation

- Isolate sensitive applications, when necessary, to prevent unauthorised access.

11.7 Mobile Computing and Teleworking

11.7.1 Mobile Device Management

- Develop and enforce policies for secure use of mobile devices, including encryption.
- Ensure that mobile devices comply with the same security standards as in-house devices.

11.7.2 Teleworking Security

- Implement secure teleworking practices, including home networks, company-approved devices, and software.
- Provide guidance and training to teleworkers on maintaining the security of remote working environments.

12 Information Systems Acquisition, Development, and Maintenance

This section outlines the security considerations that NODA must address during the acquisition, development, and maintenance of its information systems. Ensuring security at these stages is crucial for protecting data throughout its lifecycle.

12.1 Security Requirements of Information Systems

12.1.1 Security Specifications

- Include security requirements in the specifications for new information systems or enhancements to existing systems.
- Assess potential security impacts in the early stages of system development.

12.1.2 Integration into Existing Systems

- Ensure new systems are compatible with existing security policies and controls.
- Perform rigorous testing when integrating new systems with current ones.

12.2 Free and Open Source Software Use

12.2.1 Evaluation and Approval of Open Source Software

- Implement a policy favouring the evaluation and adoption of free and open-source software solutions over proprietary ones, considering their alignment with our security and operational standards.
- Undertake thorough assessments to ensure these Open Source solutions meet our stringent security requirements and offer operational benefits.

12.2.2 Management of Vulnerabilities in Open Source Software

- Regularly monitor and address vulnerabilities in Open Source and Free Software, prioritising these solutions for adaptability and community-driven security enhancements.
- Stay committed to keeping these software solutions updated, leveraging the collective expertise of the Open Source community for robust security.

12.2.3 Integration of Open Source Software

- Encourage the integration of Open Source software into our systems, aiming to provide maximum flexibility and avoid vendor lock-in for our operations and clients.
- Establish procedures that ensure the smooth integration of these solutions, reinforcing our commitment to open standards and interoperability.

12.2.4 Contributions to Open Source Projects

- Foster a culture of contributing to the Open Source community, aligning with our open innovation and collaboration philosophy.
- Our contributions to Open Source projects will enhance these projects and ensure our clients benefit from solutions free from restrictive vendor lock-ins.

12.3 Security in Development and Support Processes

12.3.1 Secure Development Policy

- Adopt and enforce a secure development policy for any in-house developed software.
- Ensure development teams are trained in secure coding practices.

12.3.2 Technical Review of Applications

- Conduct regular security reviews and audits of applications during their development life cycle.
- Utilise automated tools for code scanning and vulnerability assessment.

12.4 Technical Vulnerability Management

12.4.1 Vulnerability Assessment and Management

- Implement a process for the regular assessment, reporting, and remediation of technical vulnerabilities.
- Prioritise vulnerabilities based on their potential impact and exploitability.

12.4.2 Patch Management

- Develop a patch management policy to ensure timely application of security patches.
- Regularly review and test patches before deployment in the production environment.

12.5 Supplier Relationships

12.5.1 Supplier Security Policy

- Include security requirements in contracts and agreements with suppliers and third-party service providers.
- Ensure suppliers comply with NODA's security policies and standards.

12.5.2 Supplier Assessment

- Conduct regular assessments of suppliers to evaluate their compliance with security requirements.
- Include the right to audit clauses in contracts where necessary.

12.5.3 Information Sharing

- Establish procedures for securely sharing information with suppliers while protecting sensitive and proprietary company data.
- Define responsibilities and contact points for reporting and managing security incidents involving suppliers.

By integrating security considerations into acquiring, developing, and maintaining its information systems, NODA can better protect its assets and data from evolving threats and vulnerabilities. This approach is essential for preserving information's confidentiality, integrity, and availability throughout its lifecycle.

13 Information Security Incident Management

Prompt and effective management of information security incidents is vital for NODA to mitigate their impact and swiftly recover. This section details our streamlined incident response and reporting procedures, which are suitable for our business size and scope.

13.1 Reporting Information Security Events and Weaknesses

13.1.1 Efficient Reporting Process

- Set up a straightforward and user-friendly process for team members and stakeholders to report security concerns and weaknesses.
- Implement regular, concise training sessions to emphasise the importance of timely incident reporting.

13.1.2 Categorizing Security Events

- Develop a simple method to categorise incidents by their impact and severity.
- Create a clear escalation protocol based on these categories, ensuring an appropriate response.

13.2 Effective Management of Security Incidents

13.2.1 Specialized Response Team

- Assemble a small, flexible incident response team with diverse technical, legal, and communication expertise.

13.2.2 Dynamic Response Planning

- Craft a flexible incident response plan that covers various incident scenarios.
- Regularly review and rehearse the plan to keep it practical and relevant.

13.2.3 Incident Analysis for Improvement

- Post-incident, conduct thorough analyses to understand causes and assess response efficacy.

- Maintain an incident log for future reference and continuous learning.

13.2.4 Commitment to Improvement

- Leverage lessons learned from incidents to refine security practices and response strategies.
- Periodically update security policies and training materials in line with these improvements.

13.2.5 Transparent Communication

- Establish clear guidelines for communicating about incidents internally and, when necessary, externally.
- Prioritise transparency while respecting privacy and confidentiality in all communications.

13.2.6 Adherence to Legal Standards

- Ensure all incident management practices comply with pertinent legal and regulatory requirements, including GDPR.
- Stay informed about changes in legal standards to maintain compliance.

Through these targeted incident management strategies, NODA aims to manage security incidents effectively, minimising their impact on our operations and maintaining our reputation for swift, responsible handling of security matters.

14 Business Continuity Management

Maintaining operational continuity and minimising disruptions in the face of incidents is vital for NODA. This section delineates our approach to Business Continuity Management (BCM), emphasising the role of information security within this framework.

14.1 Integrating Information Security into BCM

14.1.1 Ensuring Security in Continuity Plans

- Seamlessly incorporate information security measures into our BCM procedures, ensuring data protection even during disruptions.
- Adapt security controls to suit alternative operating conditions under our business continuity plans.

14.1.2 Role-Based Training in BCM

- Provide targeted training for team members on their specific responsibilities in business continuity, focusing on how these responsibilities intersect with information security.
- Regularly conduct practical drills to gauge and enhance our preparedness.

14.2 Risk Assessment in Business Continuity

14.2.1 Identifying and Assessing BCM Risks

- Conduct a focused risk assessment to identify threats to our operations, particularly information security risks.
- Rank business processes and information assets based on their criticality to our operations.

14.2.2 Business Impact Analysis

- Conduct a Business Impact Analysis to understand the potential consequences of disruptions and guide the formulation of effective continuity strategies.

14.3 Developing and Implementing BCM Plans

14.3.1 Crafting Practical Continuity Plans

- Formulate concise business continuity plans that outline steps to maintain or swiftly restore key business processes and IT functions in an emergency.
- Ensure these plans include clear guidelines for data access and IT service restoration.

14.3.2 Regular Plan Testing and Refinement

- Periodically test and refine these plans to ensure they are up-to-date and effective.
- Use insights from these tests and real-life incidents to improve our response strategies continuously.

14.4 Establishing a BCM Framework

14.4.1 Building a Robust BCM Structure

- Develop a BCM framework that complements our overall risk management and information security posture.
- Assign and communicate BCM responsibilities clearly within the team.

14.4.2 Commitment to Ongoing Improvement

- Foster a culture of continuous improvement, regularly revisiting and enhancing our BCM framework to align with evolving business needs and external changes.

14.4.3 Collaborative Planning with External Entities

- Engage actively with external partners, suppliers, and emergency services in our business continuity planning.
- Account for dependencies on these external parties within our continuity strategies.

BCM at NODA is about being proactive and resilient, ensuring we are equipped to handle disruptions while safeguarding the integrity of our information assets. Integrating information security into our BCM processes is crucial for the robustness and sustainability of our business operations.

15 Compliance

For NODA, adhering to legal, regulatory, and contractual requirements, especially information security, is essential for our operations and integrity. This section highlights how we achieve and maintain compliance.

15.1 Legal and Contractual Requirements

15.1.1 Keeping Up with Laws and Regulations

- Actively stay updated on and comply with Swedish and EU laws and regulations pertinent to information security and data protection, including the GDPR.
- Regularly revisit and update our security policies to align with these evolving legal standards.

15.1.2 Fulfilling Contractual Security Obligations

- Carefully review our security commitments in contracts with clients, suppliers, and partners, ensuring they are realistic and manageable for our business size.
- Incorporate contract clauses that reflect our commitment to security and data protection while safeguarding our business interests.

15.2 Protection of Records

15.2.1 Efficient Record Management

- Maintain well-organised records of our data processing activities, including handling, transferring, and deleting data.
- Secure these records against unauthorised access or tampering.

15.2.2 Data Retention and Secure Disposal

- Adopt a data retention policy that meets both our business needs and legal requirements.
- Follow secure methods for disposing of no longer required data, ensuring complete and irreversible data erasure.

15.3 Data Protection and Privacy

15.3.1 Upholding Data Privacy

- Adhere to GDPR and other relevant privacy regulations in managing personal information.
- Develop clear data protection policies, including protocols for handling data breaches and transferring data.

15.3.2 Data Protection Officer Role

- Evaluate the need for a Data Protection Officer based on our data processing activities and appoint one, if necessary, to oversee compliance with data protection laws.

15.4 Intellectual Property Rights

15.4.1 Safeguarding Intellectual Property

- Respect and comply with laws related to intellectual property, including copyrights and patents.
- Actively protect our intellectual assets through both legal and technical means.

15.5 Security Reviews

15.5.1 Conducting Security Audits

- Regularly perform security audits to ensure we meet internal policy standards and external regulatory demands.
- Utilise audit findings to continuously enhance our security practices.

15.5.2 Ongoing Compliance Monitoring

- Monitor how effectively we meet our compliance obligations.
- Keep management and relevant stakeholders informed about our compliance status.

15.5.3 External Audits

- When appropriate, engage independent auditors to provide an external perspective on our compliance and security posture.

In our business environment, compliance is not just a legal requirement; it's a cornerstone of our trustworthiness and reputation. To ensure our clients and partners ' security and confidence, NODA is dedicated to maintaining high compliance standards, particularly in information security and data protection.

16 Policy Adoption

Adopting this Information Security Policy is crucial in safeguarding NODA's information assets and ensuring a secure and compliant operational environment. This section outlines the policy's approval, dissemination, enforcement, review, and evaluation processes.

16.1 Approval and Implementation

16.1.1 Policy Approval

- NODA's senior management must approve the Information Security Policy, ensuring it aligns with the business strategy and legal obligations.
- Secure formal sign-off on the policy from authorised executives, such as the CEO, CSIO or CTO.

16.1.2 Implementation Strategy

- Develop an implementation strategy that includes assigning responsibilities, establishing timelines, and allocating necessary resources.
- Clearly define a realistic and manageable timeline for implementing new policies or updates once approved. This timeline should account for all necessary training, adjustments in operations, and deployment of resources.
- Ensure that all employees are informed about the policy and its relevance to their roles, including the timeline for changes to be fully adopted.

16.2 Dissemination of the Policy

16.2.1 Communication with Employees

- Communicate the policy to all employees through multiple channels, such as e-mail, internal portals, or staff meetings.
- Make the policy accessible to all staff through the company intranet.

16.2.2 Training and Awareness

- Provide training and awareness programs to help employees understand the policy and their responsibilities in upholding it.

- Include information security as part of the onboarding process for new employees.

16.3 Policy Enforcement

16.3.1 Compliance Obligations

- Make compliance with the Information Security Policy a condition of employment, subject to disciplinary action for non-compliance.
- Implement monitoring and enforcing compliance mechanisms, such as regular audits and reviews.

16.3.2 Incident Handling

- Establish procedures for handling policy violations, including investigation processes and disciplinary actions.

16.4 Policy Review and Evaluation

16.4.1 Regular Review

- Review the Information Security Policy at least annually or following significant changes in the business or technological landscape.
- Ensure the policy remains relevant, effective, and aligned with current risks and regulatory requirements.

16.4.2 Continuous Improvement

- Encourage feedback on the policy from employees and stakeholders to identify areas for improvement.
- Update the policy to reflect new threats, business practices, or technological advancements.

The successful adoption and implementation of the Information Security Policy are fundamental to protecting NODA's information assets and overall security posture. Through the continuous review, evaluation, and adaptation, the policy will remain a living document that effectively guides the organisation's security efforts.

17 Appendix A: Glossary of Terms

- **Access Control**: In physical and information security contexts, access control is the selective restriction of access to a place or resource. The process involves managing who or what is allowed to enter or use a resource and is closely tied to authorisation, which is the permission to access the resource. Electronic access control (EAC) uses computers to overcome the limitations of mechanical locks and keys, allowing access based on the credentials presented. When access is granted, the door unlocks for a set time, and the transaction is recorded; if access is denied, the door stays locked, and the attempt is recorded.
- **Asset Management**: Asset management is a systematic approach to the governance and realisation of value for which a group or entity is responsible. It applies to tangible assets (like infrastructure, buildings, or equipment) and intangible assets (such as intellectual property, goodwill, or financial assets). The process involves developing, operating, maintaining, upgrading, and disposing of assets most cost-effectively, considering all costs, risks, and performance attributes.
- **Business Continuity Management (BCM)**: Business continuity refers to an organisation's ability to continue delivering products or services at acceptable predefined levels following a disruptive incident. Business continuity planning involves creating systems of prevention and recovery to address potential threats to a company. The goal extends beyond prevention to ensuring ongoing operations before and during disaster recovery execution, aiming for business continuity as the outcome of proper execution of business continuity planning and disaster recovery.
- **Change Management**: Change management involves preparing, supporting, and helping individuals, teams, and organisations make organisational changes. It encompasses methods that significantly alter a company's use of resources, business processes, budget allocations, or other operational modes. Organisational Change Management (OCM) focuses on the entire organisation and the changes it needs to make. In contrast, change management may solely refer to how such transitions impact people and teams. It involves various disciplines, from behavioural and social sciences to information technology and business solutions.
- **Data Loss Prevention (DLP)**: Data loss prevention software is designed to prevent potential data breaches or exfiltration transmissions. It works by monitoring, detecting, and blocking sensitive data while it is in use (endpoint actions), in motion (network traffic), and at rest (data storage).
- **Encryption**: In cryptography, encryption is information encoding. This process transforms the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Only authorised parties should be able to decipher a ciphertext back

to plaintext and access the original information. While encryption does not prevent interference, it denies the intelligible content to potential interceptors.

- **General Data Protection Regulation (GDPR)**: The GDPR is a regulation in the European Union on information privacy. It's a significant component of EU privacy and human rights law, particularly aligning with Article 8(1) of the Charter of Fundamental Rights of the European Union. It governs the transfer of personal data outside the EU and EEA areas. The GDPR aims to enhance individuals' control over their personal information and simplify international business's regulatory environment, replacing the earlier Data Protection Directive 95/46/EC.
- **Incident Management**: Incident management refers to the activities of an organisation to identify, analyse, and correct hazards to prevent future occurrences of incidents. An incident in this context is an event that could lead to the loss of or disruption to an organisation's operations, services, or functions. Effective incident management involves structured responses by either an incident response team (IRT), an incident management team (IMT), or an Incident Command System (ICS). The goal is to minimise the impact of incidents on business operations and vital functions.
- **Information Security (InfoSec)**: Information security, or InfoSec, protects information by mitigating information risks. It is a part of information risk management. It typically involves preventing or reducing the chance of unauthorised or inappropriate access to data and unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. The primary focus of information security is the balanced protection of data confidentiality, integrity, and availability (known as the "CIA" triad) while ensuring efficient policy implementation and organisational productivity.
- **Malware**: Malware, short for malicious software, refers to any software intentionally designed to cause damage to a computer, server, client, or computer network. This includes many harmful programs such as viruses, worms, trojan horses, ransomware, spyware, and adware. Malware acts against the interests of the computer user and typically requires some form of legitimate user action to infect or propagate.
- **Network Segmentation**: Network segmentation involves dividing a computer network into smaller parts or segments, each acting as a separate network, to improve security and performance. This practice limits the spread of network breaches by isolating them within one segment, thereby protecting the rest of the network.
- **Patch Management**: Patch management is the process of distributing and applying updates to software. These patches are often necessary to correct security vulnerabilities and other bugs. Effective patch management ensures that computers and applications are up-to-date and protected against known vulnerabilities.
- **Physical Security**: Physical security protects building sites and equipment from theft, vandalism, natural disasters, manufactured catastrophes, and accidental damage. It involves

using multiple interdependent systems, including CCTV surveillance, locks, access control protocols, and barriers.

- **Risk Management**: Risk management in information security involves identifying, assessing, and controlling threats to an organisation's digital assets. This includes analysing the risk to information systems and data and implementing strategies to mitigate these risks.
- **User Access Management (UAM)**: User Access Management is the process of defining and managing individual network users' roles and access privileges. It involves the administration of users, including authentication, authorisation, roles, and privileges within or across system and enterprise boundaries.
- **Vulnerability Assessment**: Vulnerability assessment in information security is the process of identifying, quantifying, and prioritising (or ranking) the vulnerabilities in a system, such as in software or a network.
- **VPN (Virtual Private Network)**: A VPN extends a private network across a public network, enabling users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. It provides online privacy and anonymity by creating a private network from a public internet connection.

18 Appendix B: Reference Documents

TODO

- **Software Development Guidebook**: A comprehensive resource providing practical guidelines and best practices for secure software development, aligned with NODA's IT Security Policy.
- System Architect Guidebook
- System Operator Guidebook
- Security Audit Checklist
- Incident Response and Reporting Procedures
- User Acknowledgment Form