YourIT!
Your Logo Goes Here

EU NIS2 Directive

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

25	Article 23(4)(c) - Reporting obligations - Incident intermediate report submission
26	Article 23(4)(d) - Reporting obligations - Incident final report submission
27	Article 23(4)(e) - Reporting obligations - Ongoing incident reporting

Purpose

This policy applies to the workforce members of essential or important entities operating within the scope of the business entities to which the EU NIS2 Directive regulations apply.

Scope

The EU NIS2 Directive applies to any business entity where the entity is within the scope of sectors set forth in the Directive (EU) 2022/2555 regulations and directive's Annex I - Sectors of High Criticality and Annex II - Other Critical Sectors.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

Article 20(1) - Governance - Entity management approval, oversight, and infringement liabilities associated with cyber risk-management measures

EU NIS2 Directive	Other Requirements
Article 20(1) Governance - Entity management approval, oversight, and infringement liabilities associated with cyber risk-management measures	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

Guidance
To comply with EU NIS2 Directive Article 21(1), management bodies of essential and important entities must approve, oversee, and be held accountable for cybersecurity risk-management measures.

Procedure Steps

1. Approval of Measures - Ensure that the management body formally reviews and approves all cybersecurity risk-management measures taken by the entity to comply with Article 21.

2. Oversight Responsibilities - Establish clear oversight responsibilities within the management body to monitor the implementation and effectiveness of cybersecurity measures.

3. Accountability Framework - Develop an accountability framework that outlines the management body's liability for any infringements of Article 21, ensuring they understand their legal obligations.

4. Regular Reporting - Implement regular reporting mechanisms to keep the management body informed of the status and effectiveness of cybersecurity measures.

5. Training for Management - Provide cybersecurity training for the management body to ensure they are equipped to understand and make informed decisions about risk-management measures.

6. Compliance Monitoring - Monitor compliance with Article 21 continuously, ensuring that the management body is aware of any potential issues and takes action promptly.

7. Documentation and Records - Maintain detailed records of all decisions, approvals, and actions taken by the management body concerning cybersecurity risk management.

8. Legal Alignment - Align the accountability measures with national laws regarding the liability of public institutions, servants, and officials, ensuring compliance with broader legal frameworks.

Assessment Guidance:

Periodically review entity artifacts containing the following information.

1. Measurement Report
2. Internal Audit Report
3. Management Review Minutes

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CC2.3 - Security Official: Identify the security official who is responsible for the development and implementation of the security policies and procedures.

  Procedure
  - Appoint a specific individual to take responsibility for identifying processes and tools that will be used to support the organization's cybersecurity policies.

- CC2.4 - Workforce Cybersecurity Roles & Responsibilities: Establish and document cybersecurity roles and responsibilities within the workforce.

  Procedure
  - Work with department heads and Subject Matter Experts to determine the roles of each user, and document how each role should take responsibility for the protection of organizational data. These must align with all compliance requirements.

- CC2.5 - Third-Party Cybersecurity Roles & Responsibilities: Establish and document cybersecurity roles and responsibilities with third-party stakeholders.

  Procedure
  - Work with department heads and Subject Matter Experts to determine the cybersecurity roles of each third-party vendor, and document how each vendor should take responsibility for the protection of organizational data. These must align with all compliance requirements.

- CC2.6 - Workforce Compliance Roles & Responsibilities: Establish compliance roles and responsibilities within the workforce.

  Procedure
  - Work with department heads and Subject Matter Experts to determine the compliance roles of workforce members, and document how each workforce member should take responsibility for compliance.

- CC2.7 - Third-Party Compliance Roles & Responsibilities: Establish compliance roles and responsibilities with third-party stakeholders.

Procedure
- Work with department heads and Subject Matter Experts to determine the compliance roles of each third-party stakeholders, and document how each should take responsibility for compliance.

- CC2.8 - Roles & Responsibilities Coordination: Coordinate and align information security roles & responsibilities with internal roles and external partners.

  Procedure
  - Those responsible for information security should interface with department heads, subject matter experts, executives, and third-party stakeholders. Roles should be determined and agreed to prior to incidents to facilitate an orderly response.

- CC2.10 - Agreement Compliance Validation: Periodically validate that third-parties are living up to their contracted requirements.

  Procedure
  - Questionnaires and site visits can be used to validate third-party adherence to the organization's security requirements.

- CC2.11 - Detection Roles & Responsibilities: Ensure that roles and responsibilities for detection are well defined to ensure accountability.

  Procedure
  - Identify roles and assign responsibilities for ensuring detection tools are being used, that alerts are reviewed, and incidents managed according to organizational policies.

- CC2.14 - Senior Executives: Ensure senior executives understand roles & responsibilities.

  Procedure
  - Include senior executives in all workforce cybersecurity training.
  - Perform or find executive-level training specific to senior executives that explain cybersecurity and compliance concepts; risks of downtime, regulatory penalties, reputational damage, career damage; and what executives must to do provide resources and oversight for a robust cybersecurity and compliance program.

- CC2.15 - Physical Security Personnel: Ensure physical security personnel understand their roles & responsibilities and are trained to perform them.

  Procedure
  - Train guards, facility maintenance personnel, HR, and others responsible for protecting facilities, maintaining security devices, and managing keys and access cards, to properly perform their duties.

- CC2.16 - IT Security Personnel: Ensure information security personnel understand their roles & responsibilities and are trained to perform them.

  Procedure
  - Train IT security personnel, and ensure outsourced vendors are properly trained, to perform their duties as required. Training can come from security organizations, training companies, or product vendors.

- CC3.1 - Legal and Regulatory Requirements: Identify and manage all legal and regulatory requirements.

  Procedure

  - Ask a series of questions to identify all the compliance requirements facing an organization. Some requirements may be obvious, based on the type of organization. Others may be hidden, such as contractual obligations and insurance requirements.

- CC3.2 - Governance & Risk Management Processes: Ensure governance and risk management processes address cybersecurity risks.

  Procedure
  - Align all processes to both the organization's cybersecurity and compliance requirements.

- CC5.3 - Risk Management/Mitigation: Implement security measures sufficient to mitigate or reduce risks and vulnerabilities to a reasonable and appropriate level.

  Procedure
  - Address your risks.

- CC17.10 - Risk Tolerance: Organization risk tolerance is determined and clearly expressed.

  Procedure
  - Determine the organization's risk tolerance while complying with all regulatory and legal requirements.

- CC17.11 - Risk Tolerance Alignment: Risk management aligns with all legal and regulatory requirements, the organization's role in critical infrastructure, and a sector-specific risk analysis.

  Procedure
  - Ensure all risk management activities are in compliance with regulatory and legal requirements.

- CC17.12 - Newly-Identified Vulnerabilities: Ensure that newly identified vulnerabilities are mitigated or documented as accepted risks.

  Procedure
  - Stay up to date with newly-identified technical vulnerabilities.
  - Stay up to date with new threats, including weather, civil unrest, disaster warnings, that can impact the organization's critical functions and staff.

- CC18.16 - Detection Compliance: Ensure that detection activities comply with all applicable requirements.

  Procedure
  - Verify that detection activities comply with organizational needs and regulatory and legal requirements.

- NIS2-Art 21(2)(d) - Supplier and Service Provider Agreements: Sign agreements that conform with all business and regulatory requirements ensuring suppliers and services providers protect data and network access.

  Procedure
  - Contracts including cyber risk-management measures and significant incident reporting requirements should be executed with all suppliers and service providers. EU NIS2 requires that agreements between the essential or important entity and their suppliers and/or service providers include terms addressing the cyber risk-management measures and significant incident reporting to be undertaken by suppliers and service providers in compliance with the relevant EU NIS2 Directive regulations.

References

- Article 21 of the Directive (EU) 2022/2555 of the European Parliament on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.333.01.0080.01.ENG&toc=OJ:L:2022:333:TOC#d1e3337-80-1
- Ireland National Cyber Security Centre - NIS2 A Quick Reference Guide - https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf
- Centre for Cybersecurity Belgium - NIS 2 Directive - What Does It Mean to My Organization - https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

Article 20(2) - Governance - Entity management and employee training in cybersecurity risk assessment and management practices

EU NIS2 Directive	Other Requirements
Article 20(2) Governance - Entity management and employee training in cybersecurity risk assessment and management practices	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Guidance
To comply with EU NIS2 Directive Article 20(2), essential and important entities must ensure that management bodies and employees receive ongoing training to effectively identify and manage cybersecurity risks.

Procedure Steps

1. Mandatory Management Training - Require members of management bodies to undergo mandatory cybersecurity training to equip them with the knowledge and skills to identify and assess cybersecurity risks.

2. Regular Employee Training - Encourage essential and important entities to provide regular cybersecurity training for all employees, emphasizing risk identification and the impact of cybersecurity on service continuity.

3. Customized Training Programs - Design customized training programs that address the specific cybersecurity challenges and operational needs of the entity.

4. Skill Development Focus - Ensure that training includes key areas such as threat detection, risk management, and incident response to build relevant skills.

5. Continuous Education - Promote continuous education by offering regular updates on new cybersecurity threats, technologies, and best practices.

6. Evaluation and Certification - Incorporate assessments and certifications within the training program to validate the knowledge and skills acquired by participants.

7. Monitoring Training Effectiveness - Regularly monitor and assess the effectiveness of training programs through feedback, performance metrics, and post-training evaluations.

8. Documentation and Compliance - Maintain detailed records of all training activities, including participant attendance, content covered, and assessment outcomes, to ensure ongoing compliance and track progress.

Assessment Guidance:

Periodically review entity artifacts containing the following information.

1. Training and awareness plan
2. Training records

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CC16.1 - Workforce Training: Implement workforce training that covers all required policies and procedures.

  Procedure
  - Conduct workforce training at the time of hire and regularly afterwards. Ensure all workforce members, including executives and contractors, complete their training.
  - Supplement packaged training programs with customized training focused on your unique environment, for example, the keyword that should be entered in an email subject line to send an encrypted message. Include requirements for security of work-from-home environments, secure connecting from public networks, etc.

- CC16.2 - Awareness: Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

  Procedure
  - Use signage, emails, pop-up banners, and other methods to continually remind workforce members to be diligent about cybersecurity. Topics can include phishing scams, insider and visitor threats, and storing data in secure locations.

- CC16.3 - Track Training: Implement a documented tracking system to ensure and record that all workforce members have received training.

  Procedure
  - Create written documentation of training activities so you are prepared for an audit, investigation, or lawsuit. Review the records to identify anyone not receiving required training.

- CC16.4 - Track Awareness Activities: Document awareness activities to be prepared for an audit or investigation.

  Procedure
  - Unlike training systems that automatically record training activity, or sign-in sheets for live training, you should use a calendar, ticketing system, or create documents identifying your awareness activities, including start- and end-dates, type of media, intended audience, and your message(s).

- CC16.5 - Insider Threat Training: Provide security awareness training on recognizing and reporting potential indicators of insider threat.

  Procedure
  - Train all workforce members to identify potential insider threats by other workforce members, visitors, or contractors who may try to steal data or sabotage systems.

References

- Article 21 of the Directive (EU) 2022/2555 of the European Parliament on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.333.01.0080.01.ENG&toc=OJ:L:2022:333:TOC#d1e3337-80-1
- Ireland National Cyber Security Centre - NIS2 A Quick Reference Guide - https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf
- Centre for Cybersecurity Belgium - NIS 2 Directive - What Does It Mean to My Organization - https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

Article 21(1) - Network and Information Systems - Risk Management

EU NIS2 Directive	Other Requirements
Article 21(1) Network and Information Systems - Risk Management	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Guidance
To comply with EU NIS2 Directive Article 21(1), essential and important entities must implement proportionate measures to manage risks to network and information systems, minimizing the impact of incidents and ensuring service continuity.

Procedure Steps

1. Risk Assessment - Conduct thorough risk assessments to identify vulnerabilities and potential threats to network and information systems, considering the entity's size and risk exposure.

2. Technical Measures - Implement principle of least privilege and state-of-the-art technical solutions, such as firewalls, intrusion detection systems, and encryption, to protect against identified risks.

3. Operational Measures - Establish operational practices like regular system updates, patch management, and continuous monitoring to prevent security breaches.

4. Organizational Measures - Develop organizational policies, including incident response plans, business continuity plans, and data protection policies, to manage security risks effectively.

5. Compliance with Standards - Align security measures with relevant European and international standards to ensure best practices are followed.

6. Cost-Benefit Analysis - Evaluate the cost of implementing security measures against the potential impact of security incidents to ensure proportionality and effectiveness.

7. Regular Review and Update - Periodically review and update security measures to adapt to new threats and technological advancements.

8. Training and Awareness - Provide ongoing training and awareness programs to ensure all personnel are knowledgeable about security risks and practices.

Assessment Guidance:

Periodically review entity artifacts containing the following information.

1. Risk Treatment Table
2. Risk Treatment Plan
3. Risk Assessment Methodology
4. Risk Assessment Table
5. Plan of Actions

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CC3.2 - Governance & Risk Management Processes: Ensure governance and risk management processes address cybersecurity risks.

  Procedure
  - Align all processes to both the organization's cybersecurity and compliance requirements.

- CC4.8 - Security Control Effectiveness: Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

  Procedure
  - Review security regularly because vulnerabilities and threats change.

- CC5.1 - Risk Assessment/Risk Analysis: Periodically conduct an accurate and thorough assessment of the risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of data.

  Procedure
  - Conduct a comprehensive, accurate and thorough risk assessment/HIPAA Security Risk Analysis.
  - Bring in an independent expert to perform your risk assessment without any conflict of interest.

- CC5.2 - Prioritize Risks: Prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.

  Procedure
  - Prioritize the risks identified in the Risk Analysis.

- CC14.10 - Likelihood Analysis: Determine the likelihood of an incident based on historical information and other resources.

  Procedure

  - Review disasters, weather events, cyber threats, and other information to try to determine the likelihood that an incident will happen.
  - Utilize a certified professional.

- CC17.6 - Threat and Vulnerability Information: Receive and respond to threat and vulnerability information from information sharing forums and sources and communicate to stakeholders.

  Procedure
  - Subscribe to information services, and review their notices to quickly identify vulnerabilities and threats.

- CC17.9 - Risk Management: Establish and manage risk management processes as agreed to by organizational stakeholders.

  Procedure
  - Manage risks based on organizational priorities and regulatory and legal requirements.

- NIS2-Art 21(1).Plan - Security Plans of Action: Develop and implement plans of action with timelines designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

  Procedure
  - Use written Plan of Actions and Milestones for identifying controls and practices that have not been fully implemented necessary to manage identified risks, and the timeline for remediation.

References

- Article 21 of the Directive (EU) 2022/2555 of the European Parliament on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.333.01.0080.01.ENG&toc=OJ:L:2022:333:TOC#d1e3337-80-1
- Ireland National Cyber Security Centre - NIS2 A Quick Reference Guide - https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf
- Centre for Cybersecurity Belgium - NIS 2 Directive - What Does It Mean to My Organization - https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

Article 21(2)(a) - Measures - Policies on risk analysis and information system security

EU NIS2 Directive	Other Requirements
Article 21(2)(a) Measures - Policies on risk analysis and information system security	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

2. The measures referred to in Article 21 paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

Guidance
To comply with the EU NIS2 Directive on risk analysis and information system security, important entities should develop policies that address potential threats to both digital and physical environments. These policies should take a comprehensive all-hazards approach, accounting for cyber threats, physical breaches, natural disasters, and other potential incidents.

Procedure Steps

1. Risk Analysis Framework - Develop a framework for identifying, assessing, and prioritizing risks to network and information systems.

2. Risk Assessment - Conduct regular risk assessments to evaluate both digital and physical threats.

3. Vulnerability Management - Implement a systematic process to identify, classify, and address vulnerabilities in the network and information systems. Regularly scan and assess systems for vulnerabilities, and apply timely updates and patches to mitigate potential exploits.

4. Security Policy Development - Create policies covering access control, data protection, and incident response, tailored to your specific risks.

5. Implementation and Training - Implement the policies and conduct training for stakeholders to ensure adherence.

6. Monitoring and Review - Establish a monitoring mechanism and conduct periodic reviews to adapt to evolving threats.

Assessment Guidance:

Periodically review entity artifacts containing the following information.

1. Policy on Information Security
2. Records of Policy on Information Security Changes

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CC7.2 - Physical Access Management: Manage and protect physical access to assets.

  Procedure
  - Use locks, guards, and other measures to block visitors and unauthorized staff members from getting to devices.

- CC7.17 - Escort & Monitor Visitors: Escort visitors and monitor visitor activity.

  Procedure
  - Visitors should be escorted and monitored to ensure they do not attempt to access organizational systems.

- CC7.18 - Facility Security Plan: Implement documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

  Procedure
  - An overall security plan should be written defining layers of physical security, including alarms, locks, surveillance, guards, signage, etc.

- CC7.19 - Physical Access Devices: Control and manage physical access devices.

  Procedure
  - Keys and electronic keycards should be carefully controlled and managed, including inventories, lists, signed acknowledgements, immediate response when one is lost, and retrieval upon termination.

- CC7.20 - Physical Access Logs: Maintain audit logs of physical access.

  Procedure
  - Alarm and locking system logs, and sign-in sheets, should be retained for audits and investigations.

- CIS1.1 - Establish and Maintain Detailed Enterprise Asset Inventory: Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

- CIS1.2 - Address Unauthorized Assets: Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

- CIS2.1 - Establish and Maintain a Software Inventory: Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.

- CIS2.2 - Ensure Authorized Software is Currently Supported : Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

- CIS2.3 - Address Unauthorized Software: Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

- CIS3.1 - Establish and Maintain a Data Management Process: Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS3.2 - Establish and Maintain a Data Inventory: Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

- CIS4.1 - Establish and Maintain a Secure Configuration Process: Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure: Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS7.1 - Establish and Maintain a Vulnerability Management Process: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS7.2 - Establish and Maintain a Remediation Process: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

- CIS8.1 - Establish and Maintain an Audit Log Management Process: Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS11.1 - Establish and Maintain a Data Recovery Process : Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS14.1 - Establish and Maintain a Security Awareness Program: Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS15.2 - Establish and Maintain a Service Provider Management Policy: Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS16.1 - Establish and Maintain a Secure Application Development Process: Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.4 - Establish and Maintain an Incident Response Process: Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS18.1 - Establish and Maintain a Penetration Testing Program: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

References

- Article 21 of the Directive (EU) 2022/2555 of the European Parliament on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.333.01.0080.01.ENG&toc=OJ:L:2022:333:TOC#d1e3337-80-1
- Ireland National Cyber Security Centre - NIS2 A Quick Reference Guide - https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf
- Centre for Cybersecurity Belgium - NIS 2 Directive - What Does It Mean to My Organization - https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

Article 21(2)(b) - Measures - Incident handling

EU NIS2 Directive	Other Requirements
Article 21(2)(b) Measures - Incident handling	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The measures referred to in Article 21 paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(b) incident handling;

Guidance
To comply with EU NIS2 Directive Article 21 on incident handling, entities should establish procedures for preparing for, detecting, responding to, and recovering from incidents. This includes a comprehensive incident response plan, detection systems, communication protocols, and post-incident analysis.

Procedure Steps

1. Develop Incident Response Plan - outline procedures and roles for handling incidents.

2. Implement Detection and Reporting - Set up systems to detect and report incidents early.

3. Coordinate Response - Ensure team coordination and assign clear responsibilities.

4. Containment and Mitigation - Develop strategies to isolate affected systems and mitigate impacts.

5. Communication Plan - Keep stakeholders informed with clear communication protocols.

6. Recovery and Restoration - Establish procedures to restore normal operations.

7. Post-Incident Analysis - Analyse incidents to identify root causes and improve responses.

8. Training and Drills - Conduct regular training and drills to enhance preparedness.

Assessment Guidance:

Periodically review entity artifacts containing the following information.

1. Incident Management Procedure
2. Incident Log

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS8.2 - Collect Audit Logs: Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.
- CIS8.3 - Ensure Adequate Audit Log Storage: Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.
- CIS8.4 - Standardize Time Synchronization: Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.
- CIS8.5 - Collect Detailed Audit Logs: Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
- CIS8.6 - Collect DNS Query Audit Logs: Collect DNS query audit logs on enterprise assets, where appropriate and supported.
- CIS8.7 - Collect URL Request Audit Logs: Collect URL request audit logs on enterprise assets, where appropriate and supported.
- CIS8.8 - Collect Command-Line Audit Logs: Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.
- CIS8.9 - Centralize Audit Logs: Centralize, to the extent possible, audit log collection and retention across enterprise assets.
- CIS8.10 - Retain Audit Logs: Retain audit logs across enterprise assets for a minimum of 90 days.
- CIS8.11 - Conduct Audit Log Reviews: Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.
- CIS13.1 - Centralize Security Event Alerting: Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.
- CIS13.11 - Tune Security Event Alerting Thresholds: Tune security event alerting thresholds monthly, or more frequently.
- CIS17.1 - Designate Personnel to Manage Incident Handling: Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
- CIS17.2 - Establish and Maintain Contact Information for Reporting Security Incidents: Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

- CIS17.3 - Establish and Maintain an Enterprise Process for Reporting Incidents: Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.4 - Establish and Maintain an Incident Response Process: Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.5 - Assign Key Roles and Responsibilities: Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.6 - Define Mechanisms for Communicating During Incident Response: Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.7 - Conduct Routine Incident Response Exercises: Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

- CIS17.8 - Conduct Post-Incident Reviews: Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

- CIS17.9 - Establish and Maintain Security Incident Thresholds: Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

References

- Article 21 of the Directive (EU) 2022/2555 of the European Parliament on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.333.01.0080.01.ENG&toc=OJ:L:2022:333:TOC#d1e3337-80-1
- Ireland National Cyber Security Centre - NIS2 A Quick Reference Guide - https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf
- Centre for Cybersecurity Belgium - NIS 2 Directive - What Does It Mean to My Organization - https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

Article 21(2)(c) - Measures - Business continuity

EU NIS2 Directive	Other Requirements
Article 21(2)(c) Measures - Business continuity	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

The measures referred to in Article 21 paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(c) business continuity, such as backup management and disaster recovery, and crisis management;

Guidance
To comply with EU NIS2 Directive Article 21 on business continuity, entities should develop strategies for backup management, disaster recovery, and crisis management.

Procedure Steps

1. Continuity Plan - Outline procedures for maintaining essential functions.

2. Backup Management - Implement a backup strategy with secure offsite storage.

3. Disaster Recovery - Create a plan detailing recovery procedures and timelines.

4. Crisis Team - Establish a crisis management team with clear roles.

5. Communication - Develop a strategy for stakeholder communication.

6. Testing and Drills - Regularly test and conduct drills for plan effectiveness.

7. Post-Incident Review - Review and improve strategies post-incident.

8. Training - Provide training on continuity and crisis management procedures.

Assessment Guidance:

Periodically review entity artifacts containing the following information.

1. Business Continuity Plan
2. Backup Policy
3. Disaster Recovery Plan
4. Crisis Management Plan

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CIS11.1 - Establish and Maintain a Data Recovery Process : Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS11.2 - Perform Automated Backups : Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

- CIS11.3 - Protect Recovery Data: Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

- CIS11.4 - Establish and Maintain an Isolated Instance of Recovery Data : Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

- CIS11.5 - Test Data Recovery: Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

- CIS17.1 - Designate Personnel to Manage Incident Handling: Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.4 - Establish and Maintain an Incident Response Process: Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.5 - Assign Key Roles and Responsibilities: Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

- CIS17.6 - Define Mechanisms for Communicating During Incident Response: Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

References

- Article 21 of the Directive (EU) 2022/2555 of the European Parliament on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.333.01.0080.01.ENG&toc=OJ:L:2022:333:TOC#d1e3337-80-1
- Ireland National Cyber Security Centre - NIS2 A Quick Reference Guide - https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf
- Centre for Cybersecurity Belgium - NIS 2 Directive - What Does It Mean to My Organization - https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

Truncated Sample Document