Nyrstar Vendor Cybersecurity Requirement

NYRSTAR GROUP POLICY

Table of Contents

1. Purpose & Scope

This policy defines the cybersecurity requirements that Nyrstar's third-party vendors, suppliers, contractors, and service providers must meet when doing business with Nyrstar. The aim is to ensure every vendor maintains security hygiene and does not introduce avoidable cyber risks to Nyrstar's environment, in compliance with EU NIS2's broad supply chain risk management mandate.

2. Scope

The standard is divided into two sections catering to two sets of Nyrstar suppliers and vendors:

- **Section 1 - Baseline Security Requirements**: Applies to all third-party vendors, suppliers, contractors, and service providers, regardless of whether the vendor has IT system access or handles sensitive data.
- **Section 2 – Stringent Security Requirements:** Applies to vendor, supplier, or service provider that connects to Nyrstar networks, accesses Nyrstar systems or databases, handles Nyrstar's sensitive information, or supports critical infrastructure. These suppliers are categorized as **High and Medium risk** based on the risk questionnaires defined in Nyrstar Third Party Security Risk Management Policy.

3. Section 1 – Baseline Security Requirements (All Vendors)

These security requirements apply to all Nyrstar vendors, including the ones with no direct network access (e.g. providers of goods or services unrelated to IT) – for instance, a vendor's compromised email account should not become a vector for phishing Nyrstar. This baseline standard thus protects Nyrstar's overall ecosystem.

For vendors who **do** receive system access or handle sensitive data, this general standard applies **alongside** the more stringent controls of defined in **Section 2** (if both apply, the stricter requirement takes precedence).

All vendors must, at a minimum, adhere to the following cybersecurity practices:

3.1. Basic Security Governance

The vendor should have at least a minimal **information security policy or acceptable use policy** in place for its organisation. This could be as simple as documented rules or guidelines that employees must follow to keep systems secure (e.g. password rules, handling of customer data).

3.2. Legal and Regulatory Compliance

Vendors must comply with all **applicable cybersecurity laws and regulations**. This includes data protection laws (e.g. GDPR if personal data is involved) and industry standards relevant to their services.

3.3. Access Control (if applicable)

If under the contract the vendor will be given access to any Nyrstar systems, facilities, or data (even minimal, such as a secure portal or an email address for Nyrstar):

- Access will only be provisioned to authorised individuals as approved by Nyrstar, and strictly limited to what is necessary (*least privilege*).
- The vendor must ensure **no sharing of accounts or credentials**; each user must have distinct login details if accounts are provided. For example, if a vendor technician gets a temporary badge to enter a Nyrstar site, they should not loan it to anyone else.

3.4. Vendor Personnel Device Security

Even if a vendor does not log into Nyrstar computers, any devices they use to interact with Nyrstar (sending emails, accessing shared files, etc.) should be secured. This means using strong passwords, and keeping devices patched and malware-free. The goal is to ensure a compromised vendor device can't be used to attack Nyrstar.

3.5. Cyber Hygiene & Technical Controls

All vendors must practice basic cyber hygiene to protect their own IT environments, which in turn protects Nyrstar. Key expectations include:

- **Malware Protection:** Use reputable anti-virus/anti-malware tools on systems that may exchange data with Nyrstar.
- **System Updates:** Keep vendor systems (computers, software, network devices) up to date with security patches, especially those used in providing services to Nyrstar.
- **Secure Configuration:** Adhere to basic secure configuration practices such as using strong passwords, disabling unnecessary services, and maintaining firewalls on the vendor's own network.

3.6. Data Protection & Confidentiality

Any information that Nyrstar shares with a vendor, even if not highly sensitive, must be treated as confidential:

- Vendors must **protect Nyrstar's data** in their possession from unauthorised disclosure, alteration, or loss.
- Vendors may **not use Nyrstar data for any purpose outside the scope of their work for Nyrstar**.
- When the vendor no longer needs Nyrstar data, they should return it to Nyrstar or securely destroy it.

3.7. Personnel & Training

Vendors should ensure their employees exercise good security practices.

- Staff handling Nyrstar's business should be made aware of the importance of security and confidentiality.
- It's **recommended** that vendors provide **basic cybersecurity awareness training** to their staff at least annually, covering topics like recognizing suspicious emails and using strong passwords.

3.8. Incident Reporting

All vendors, even those without direct system access, **must notify** Nyrstar of **security incidents** that could **potentially affect** Nyrstar**.** This includes:

- If the vendor **discovers a data breach or cyber incident in their own environment that involves Nyrstar's information** (e.g. a hacker stole documents that contain Nyrstar data, or an email compromise at the vendor might have exposed correspondence with Nyrstar), they need to inform Nyrstar promptly.

- If a cyber incident at the vendor **disrupts their ability to deliver services** (for instance, a ransomware attack crippled the vendor's operations), they should inform Nyrstar of any resulting impact or delays.
- The expectation is that vendors will report such issues **without undue delay**.

4. Section 2 – Stringent Security Requirements (High and Medium Risk Vendors)

This standard defines the stringent cybersecurity controls required of any external vendor, supplier, or service provider that **connects to Nyrstar networks, accesses Nyrstar systems or databases, handles Nyrstar's sensitive information, or supports critical infrastructure**. These suppliers are categorized as High and Medium risk based on the risk questionnaires defined in Nyrstar Third Party Security Risk Management Policy.

It ensures that such High and Medium risk vendors maintain security measures *equivalent* to Nyrstar's internal standards in order to protect Nyrstar's operations and comply with the EU NIS2 Directive's supply chain security obligations.

This includes IT/OT technology providers, cloud and software vendors, managed service providers, consultants with system access, and any third party processing confidential or operational data. These requirements are **in addition to** the **general baseline requirements (Section 1)**, reflecting the higher risk these vendors pose.

Overall Principle:

Vendors in scope **must implement robust security controls and practices at least at the level Nyrstar requires internally**. They will be subject to *risk-based due diligence and continuous oversight* by Nyrstar. Failure to meet these requirements or to remedy identified gaps may result in contract termination or other enforcement action.

The following security domains and controls **must** be addressed by the vendor:

4.1. Security Governance

The vendor shall maintain an active information security programme, including an established security policy and supporting procedures approved by its management. A dedicated security officer or team must be responsible for overseeing compliance with these requirements.

4.2. Risk Management & Protective Measures

Vendors must regularly assess cybersecurity risks within their operations, especially any risks that could impact Nyrstar's systems or data. Appropriate technical and organisational measures shall be implemented to mitigate identified risks. At minimum, the vendor is expected to:

- **Malware Protection & Patching:** Keep systems used in service delivery up-to-date and protected. This includes installing anti-malware software on relevant systems and applying critical security patches in a timely manner. The vendor's products or services **must not** rely on **obsolete or unsupported software** that could introduce security risks.
- **Network Security:** Implement network security controls such as firewalls, secure network segmentation, and intrusion detection. Remote connections into Nyrstar should pass through secure gateways (VPNs, jump hosts) as approved by Nyrstar's IT.
- **Secure Configuration:** Apply secure configuration baselines to all systems and devices used to connect to Nyrstar (disabling default passwords, unnecessary services, using strong authentication and encryption settings). Conduct vulnerability scanning and remediate any high-risk findings promptly.

4.3. Identity & Access Control

Vendors with access to Nyrstar's digital environment must enforce strict access controls:

- Access to Nyrstar systems, networks, or data must be limited to vendor personnel **authorised and required** for the contract's scope (principle of *need-to-know*). The **least privilege** principle should be applied – accounts should have the minimum rights necessary.
- **Unique Credentials:** All vendor personnel must use **individual, unique user accounts** – sharing of credentials is prohibited.
- **Multi-Factor Authentication (MFA):** The vendor **must** use multi-factor authentication for any remote access into Nyrstar systems and for any account with elevated privileges.
- **Privileged Access Management:** Any administrative or privileged access by the vendor to Nyrstar servers must be managed through Nyrstar's Privileged Access Management tool.
- Promptly remove or revoke access when a vendor staff member no longer needs it (e.g. role change or leaving the vendor's employ). The vendor should have a process to immediately inform Nyrstar of personnel changes so accounts can be disabled, preventing orphaned access.

4.4. Data Protection & Privacy

Vendors shall rigorously protect **any Nyrstar data** they handle:

- **Data Use Restrictions:** Nyrstar data may **only** be used for purposes defined in the contract. Vendors must not access, analyse, or share Nyrstar's information beyond what is authorised. Any Nyrstar-provided data must be returned or securely deleted when no longer needed.
- **Encryption:** All sensitive data **in transit** between Nyrstar and the vendor must be encrypted using strong protocols (e.g. TLS 1.2 or above for network connections). Likewise, any Nyrstar data **at rest** on vendor systems (files, databases, backups) must be encrypted with robust encryption (such as AES-256) or protected by equivalent measures.
- **Access Restriction:** The vendor must implement internal controls to prevent **unauthorised access, alteration, or loss** of Nyrstar data. This includes access control, but also monitoring access to Nyrstar data within the vendor's environment and ensuring data is not copied to uncontrolled media. If personal data is involved, GDPR requirements must also be met by the vendor.
- **Data Return/Deletion:** Upon completion of the contract or at Nyrstar's request, the vendor should securely return or erase Nyrstar's data from its systems, certifying that no copies remain, unless storage is required by law (in which case the vendor must continue to protect it).

4.5. Secure Development & System Maintenance

If the vendor provides software development (or SaaS) or manages systems for Nyrstar, the following apply:

- **Secure Development Lifecycle:** Vendors must follow secure-by-design and secure coding best practices during development. This includes threat modeling, code review, and security testing (e.g. static/dynamic analysis) as part of the SDLC.
- **Segregation of Environments:** Development, test, and production environments must be separated. Real Nyrstar data should not be used in non-production environments. If testing requires sample data, it must be anonymised or synthetic.
- **Vulnerability Management:** The vendor must monitor for and promptly remediate security vulnerabilities in any product or system they supply to Nyrstar. They should provide timely patches, updates or mitigations when new vulnerabilities are discovered. The vendor should not introduce systems that are end-of-life or unpatchable.
- **Change Management:** Any changes to the vendor's systems that could affect Nyrstar (including software updates or configuration changes) should be done through a controlled change management process with appropriate testing and notification to Nyrstar if significant.

4.6. Personnel Security

The vendor must ensure that its staff and contractors who are involved in Nyrstar's services are trustworthy and aware of security responsibilities.

- **Security Training:** Vendor personnel working on Nyrstar's account must receive regular cybersecurity awareness training.
- **Confidentiality Agreements:** All individuals handling Nyrstar data should be under appropriate confidentiality or non-disclosure agreements.

4.7. Incident Management & Notification

Vendors shall have **documented incident detection and response processes** to handle potential security breaches on their side. In the event of **any security incident** (e.g. data breach, malware outbreak, or unauthorised access) that **could impact Nyrstar's data, systems, or services**, the vendor **must notify Nyrstar immediately (without undue delay)**. Practically, this means:

- **Immediate Notification:** The vendor should inform Nyrstar as soon as an incident is confirmed, **ideally within 24 hours** of discovery. Initial notification can be high-level but should indicate the nature of the incident and any immediate known impact.
- **Incident Details & Updates:** The vendor must provide details of the incident, including what Nyrstar data or systems might be affected, as soon as that information is available.
- **Containment and Recovery:** The vendor is expected to **take immediate steps to contain** the incident and mitigate damage. They should *remediate* the root cause and verify security before resuming normal operations.
- **Collaboration:** The vendor must **cooperate fully** with Nyrstar's investigation and response efforts. This may include providing relevant log data, forensic reports, or access for Nyrstar or third-party auditors to verify the incident's scope. If needed, the vendor should agree to temporarily suspend services or disconnect from Nyrstar systems to prevent further harm.

- **Post-Incident Actions:** After resolution, the vendor should share a post-incident report with root cause analysis and corrective measures.

4.8. Ongoing Security Monitoring & Audit

Nyrstar will actively oversee the security of high risk vendors:

- **Periodic Assessments:** Vendors must accommodate **security reviews** by Nyrstar or its appointed representatives. Nyrstar reserves the right to conduct an audit **at least annually** for critical high risk vendors, which may involve on-site inspection or remote assessment of the vendor's security controls.
- **Evidence of Compliance:** Upon request, the vendor must provide evidence of its cybersecurity measures. This can include policies, penetration test results, or external certifications and audit reports (e.g. ISO 27001 certification, SOC 2 report) to demonstrate a mature security posture.
- **Remediation of Findings:** If any security gaps or non-compliance issues are identified (through an audit or incident), the vendor is expected to remediate these issues within a reasonable timeframe agreed with Nyrstar.
- **Refusal and Non-Compliance:** Refusal to participate in required assessments, or significant failures to meet these security requirements, will be considered a **breach of contract**. Nyrstar may then exercise penalties or termination clauses.

4.9. Supply Chain Security & Flow-Down

The vendor is responsible for ensuring the security of their own relevant supply chain:

- If the vendor **engages any sub-contractors or third parties** ("fourth parties") to handle Nyrstar information or to fulfil key parts of the service, the vendor **must flow down equivalent security requirements** to those parties. The vendor shall not outsource any Nyrstar-related work to sub-parties without Nyrstar's approval.
- The vendor should maintain an **updated list of subcontractors** involved in Nyrstar's project and provide it to Nyrstar upon request.
- The vendor remains **fully accountable** for any breaches or security failings of their subcontractors in relation to Nyrstar's data/systems.
- Vendors should actively manage risks posed by their suppliers. This includes ensuring that any products, software, or components they deliver to Nyrstar are sourced from reputable, secure origins (to avoid tainted hardware/software).

4.10. Documentation & Compliance Reporting

The vendor should maintain documentation proving compliance with these controls. Upon Nyrstar's request the vendor must produce documents such as:

- Information security policy and procedures.
- Risk assessment reports and risk treatment plans.
- Incident response plan and recent incident report summaries.
- Training records, audit logs, and compliance certificates.

5. Enforcement

To ensure compliance, Nyrstar enforces these requirements through vendor contracts:

- All the above requirements form part of the vendor contract. Non-compliance is treated as a breach of contract.
- **Audit and Inspection Rights:** Nyrstar retains the right to audit the vendor's compliance, as noted.
- **Penalties and Remedies:** If a vendor is found non-compliant or suffers a serious security incident due to negligence, Nyrstar may invoke penalty clauses. This can include **withholding payments, applying financial penalties, suspending the service, or ultimately terminating the contract for material breach**.
- **Termination & Exit Strategy:** Vendors providing critical services may be required to agree on an **exit strategy** in case of severe security breach or compliance failure. This ensures Nyrstar can safely transition to an alternative solution if needed. Additionally, the vendor must support continuity of service—meaning they should have recovery plans so that a cyber incident on their side does not unduly disrupt Nyrstar's operations. Failure to have or execute such plans could be considered a breach.