External Provider Standard - Cybersecurity

Document type: Guidelines

Document ID: 251729

Document classification: Public

Approval date: 07/01/2026

Table of contents

1 Introduction

Starion develops and delivers tailored system engineering services and solutions for space, defence and other critical infrastructures across Europe, and can only do so if everyone working at Starion commits to meet the standards outlined in our Starion Code of Conduct. Our Code of Conduct is underpinned by our values:

- **Integrity** – We insist on ethical conduct in all our endeavours;
- **Inspiration** – Fuelled by passion, propelling us towards excellence
- **Care** – We are committed to individual wellbeing and growth
- **Collaboration** – Generating strength from diverse perspectives through teamwork.

We recognise that any business operating today will manage data, systems and digital services and we all have a responsibility to ensure that this is done securely, responsibly and in compliance with evolving regulations. This commitment is reflected in the four pillars of our Compliance Programme:

- **Our Structure** – We meet our legal obligations to trade and operate
- **Our Operations** – From people to services…we operate with excellence
- **Our Growth** – We follow our processes, making the right decisions to grow our business
- **Our Reputation** – We act with integrity and always do the right thing.

Cybersecurity has become a critical pillar of operational resilience and regulatory compliance, especially considering evolving legislation and standards such as the **NIS2 Directive** and **ISO/IEC 27001:2022**. The NIS2 Directive imposes enhanced obligations on organisations across the European Union (EU) to safeguard digital infrastructure, ensure business continuity and manage risks – including those introduced through external providers and supply chains.

Our External Provider Standards are not designed to dictate how you operate your business; rather, they are intended to highlight the cybersecurity responsibilities that apply to you as a business generally and in support of your engagement with the Starion. It is designed to support you in assessing, reviewing and applying appropriate technical and organisational controls that help ensure your services are resilient, secure and compliant with legal and contractual expectations.

We thank you for your support of Starion and we appreciate your co-operation in helping us ensure that you, as one of our External Providers, understand and commit to the same standards as we do within Starion.

Gaëtan Desclée

CEO – Starion

2 Who does this standard apply to?

Every business must comply with its legal and regulatory obligations in respect of cybersecurity and this External Provider Standard helps guide you generally as a business to understand your obligations. However, the nature of Starion's business means that we require, in certain circumstances, to work closely with our External Providers to verify, develop and ensure that their cybersecurity measures meet Starion's obligations. This External Provider Standard applies where an External Provider:

- Accesses Starion Systems as part of the External Provider services
- Accesses Starion Data that is security classified or commercially sensitive
- Processes Personal Data on behalf of Starion
- Supports Starion's critical business operations.

As part of our relationship with you, and the services you provide to Starion, we will notify you whether the services you provide fall into the above categories and take steps to help you assess what this means for your business, and how you can comply with this External Provider Standard.

External Providers must ensure generally that they comply with legal requirements in respect of cybersecurity and, where they fall into the above categories, engage with Starion to assess, define, implement and maintain strong, risk-based cybersecurity practices that protect systems, data and services.

3 Understanding cybersecurity principles

Our organisation is committed to maintaining resilient, risk-based and accountable cybersecurity practices across all our operations, including where our operations are supported by our External Providers. The following principles guide how we protect data, manage risks and ensure continuity of service, and what we expect of our External Providers:

- **Confidentiality, integrity and availability (CIA):** Protect sensitive data from unauthorised access, ensure systems and data remain accurate and trustworthy, and maintain reliable access to systems and services
- **Risk-based approach:** Identify and assess cybersecurity risks based on business impact, apply proportionate technical and organisational controls, and continuously monitor and adapt to emerging threats
- **Defence in depth:** Use layered cybersecurity controls across endpoints, networks, applications and users, combining preventive, detective and responsive measures
- **Accountability and governance:** Assign clear roles and responsibilities for cybersecurity, maintain documented policies and audit trails, and ensure leadership oversight and Board-level engagement
- **Incident preparedness and response:** Implement detection, containment and recovery capabilities, maintain documented incident response procedures, and report incidents to Starion within 24 hours and to authorities

- **Supply chain cybersecurity:** Assess and monitor third-party providers, require contractual obligations for equivalent cybersecurity standards, and extend controls across all service delivery layers
- **Continuous improvement:** Regularly test, review and update cybersecurity measures, conduct audits and staff training, and maintain certifications or evidence of compliance (e.g. ISO 27001, SOC 2)
- **Asset management**: Maintain an inventory of information assets, classify them based on sensitivity and criticality, and apply appropriate protection measures
- **Access control and identity management**: Ensure that access to systems and data is granted based on business need, using strong authentication and authorisation mechanisms
- **Secure development and change management**: Integrate security into software development and system changes, including secure coding practices, testing and approval workflows
- **Monitoring and logging**: Implement continuous monitoring of systems and networks, maintain logs for security events, and ensure they are protected and reviewed regularly
- **Legal, regulatory and contractual compliance**: Ensure adherence to applicable laws, regulations and contractual obligations related to information security and data protection.

Starion expects External Providers to implement and maintain strong, risk-based cybersecurity practices that protect systems, data and services, aligned to the principles of confidentiality, integrity and availability.

4 Defining your technical and organisational measures

If you are a business providing services, infrastructure or technology that connects to or supports Starion's operations, you are required to implement appropriate **technical and organisational cybersecurity measures** to protect the systems, data and services you interact with. These measures must align with the principles of **confidentiality, integrity and availability**. The minimum required technical and organisational requirements are outlined below and apply to Starion, you as an External Provider and your supply chain, and should be implemented in a manner proportionate and appropriate to your business. The nature of the services you provide, and how you provide them, may require additional technical and organisational measures to be implemented, which will be agreed with you.

4.1 Required technical measures

- Use of strong authentication and role-based access controls, on a least privilege principle basis, to monitor privileged access, managing access through multi-factor authentication (MFA) and data loss prevention (DLP) measures to prevent unauthorised access or exfiltration of data
- Encryption for data in transit and at rest
- Regular patching and vulnerability management for all systems and applications
- Secure configuration and hardening of operating systems, applications and network devices

- Endpoint protection (e.g. antivirus, anti-malware, host firewalls)
- Monitoring and logging of cybersecurity events, with integration into security information and event management (SIEM) tools where applicable, and maintaining and reviewing of logs on a regular basis
- Backup and recovery procedures, tested regularly to ensure business continuity
- Asset management: All devices and systems used to deliver services must be inventoried and secured
- Data and hardware must be securely wiped or destroyed when no longer needed to prevent unauthorised recovery
- Anti-malware protection must go beyond endpoint tools and include proactive strategies such as sandboxing, threat intelligence and behavioural analysis
- Integration of cybersecurity assessment within the software development life cycle, including secure coding practices, code reviews and vulnerability scanning
- Apply network segmentation to isolate critical systems and reduce lateral movement; use firewalls, intrusion detection and prevention systems (IDS/IPS) and secure remote access
- Ensure all systems use synchronised time sources (e.g. Network Time Protocol, NTP) to maintain accurate logging and forensic traceability
- Monitor and manage system capacity to prevent performance degradation or outages that could impact availability
- Define and enforce policies and procedures for cryptographic algorithms, key management and certificate handling
- Apply cybersecurity controls for remote access, mobile devices and 'bring your own device' (BYOD), including virtual private network (VPN), device encryption and endpoint management.

4.2 Required organisational measures

- Cybersecurity awareness training for all staff involved in service delivery, and endorsement and ownership from executive management of cybersecurity requirements within your business
- Documented cybersecurity policies, incident response procedures, including communication pathways (internal and external), escalation pathways and containment protocols that are reviewed regularly
- Segregation of duties to minimise risk
- Integration of cybersecurity considerations into business decisions
- Supplier risk management processes to assess and monitor third-party cybersecurity posture
- Periodic internal audits and reviews of cybersecurity controls and compliance status, including lessons learned and continuous improvement follow-up
- Change management for systems, applications and infrastructure must follow a documented process to ensure cybersecurity and traceability

- Business continuity and disaster recovery (BC/DR): Providers must maintain documented BC/DR plans with recovery time and point objectives (RTO and RPO) aligned to service criticality, including backup, restore and failover capabilities. Plans must be tested annually, with results available upon request.

Starion requires External Providers to maintain and consistently apply documented cybersecurity measures that protect systems and data, support NIS2 and ISO27001 compliance, and extend across their supply chain. These controls must be regularly tested, monitored and updated to address evolving threats.

5 What are your roles and our roles?

Clear roles and responsibilities are essential for maintaining secure, compliant and resilient operations. Starion and its External Providers must work in partnership to uphold the standards outlined in this document.

Our External Providers must:

- Maintain secure operations across all systems, services and supply chains
- Implement appropriate technical and organisational measures to protect Starion's data and systems
- Report cybersecurity incidents, breaches or suspected vulnerabilities immediately
- Support investigations, audits and remediation activities
- Follow all instructions received to mitigate or manage cybersecurity threats and implement them within your business
- If any required cybersecurity measures cannot be implemented, engage with Starion to identify alternative controls that meet the same objectives
- Demonstrate cybersecurity assurance through certifications, audit results or documented policies.

Starion will:

- Monitor provider compliance with this Cybersecurity Standard and contractual obligations
- Provide onboarding guidance and clarification of cybersecurity expectations
- Share relevant risk information to enable ongoing cybersecurity measures to be assessed
- Coordinate audits, reviews and incident response activities
- Engage constructively with you to resolve issues and improve cybersecurity.

We ask our External Providers to perform the obligations outlined above, and to support Starion in performing its obligations, working constructively with Starion and monitoring and continuously improving technical and organisational measures to address existing and emerging cybersecurity threats.

6 Managing your own supply chain compliance

Whether you are a service provider, technology integrator or infrastructure partner, you will operate systems internally within your organisation or outsource components and services to third parties. These third parties become your contractors or subcontractors and form part of your extended supply chain.

Systems may be owned and operated by you as an External Provider, but they often rely on third-party components, platforms or services. If you deliver services to Starion using outsourced systems, infrastructure or subcontracted support, you are responsible for ensuring that those third parties meet Starion's cybersecurity expectations.

Starion actively manages its supply chain compliance by requiring all External Providers to assess and monitor the cybersecurity measures implemented by their own vendors appropriate to the services its supply chain provides. Your contracts must include flow-down clauses applying obligations appropriate to the services provided by your own supply chain. Where parts of your supply chain support Starion's own operations, and you fall into the categories outlined above, this may include assessing and requiring additional cybersecurity measures within your supply chain on a focused basis.

Maintaining open and proactive communication, and determining and implementing appropriate measures to respond to threats is critical. Starion relies on you to engage meaningfully and be able to appropriately apply measures across your supply chain to protect Starion's systems and data.

External Providers must be able to actively manage cybersecurity within their supply chains appropriate to the criticality of the services they receive and the sensitivity of data processed, whether in support of their operations generally or specifically in support of Starion's operations. External Providers, through contractual clauses, must be able to monitor and engage their supply chains to constantly evolve cybersecurity measures.

7 What to do if there is a cybersecurity incident

In the event of a cybersecurity incident, whether actual or suspected, timely and transparent communication is essential to minimise impact and ensure coordinated response.

1. **Notification timeline:** Providers must notify Starion within 24 hours of detecting any cybersecurity incident that affects, or could potentially affect, Starion systems, data or services. This includes breaches, unauthorised access, malware infections, service disruptions or any other event that compromises confidentiality, integrity or availability.
2. **Required details:** Initial incident reports must include: the nature and scope of the incident; the systems, services and data affected; any mitigation actions taken or planned; the root cause, if known; and whether any third-party involvement or impact has been identified. Updates must be provided as new information becomes available, including resolution status and lessons learned.
3. **Coordination and support:** External Providers must fully cooperate with Starion's internal cybersecurity team by participating in investigations, supporting containment and recovery,

providing access to relevant systems and logs, and assisting with regulatory reporting and post-incident reporting and actions.

External Providers must report cybersecurity incidents within 24 hours, provide detailed and timely updates, and fully cooperate with Starion's internal teams and regulatory obligations. They are expected to act swiftly, transparently and collaboratively to contain threats, protect data and prevent recurrence.

8 Audit

Starion will need to engage with you throughout our contractual relationship to verify that you continue to implement and maintain cybersecurity measures in accordance with our contractual arrangements and this External Provider Cybersecurity Standard. There are several reasons for this requirement: it may be driven by Starion's customer obligations, external certifications or permits, applicable laws and regulations (including NIS2), or internal assurance needs.

Unless circumstances prevent it, we will always provide reasonable advance notice of any audit activities we undertake, along with the terms of reference for the audit. Audits may be conducted directly by Starion or by an authorised third party.

Audits may occur annually as part of routine assurance or on an ad hoc basis, depending on risk level, incident history or regulatory triggers. The scope may include review of your cybersecurity controls, policies, governance frameworks and logs relevant to service delivery and incident response.

Audits may identify issues, particularly risks related to how you manage and secure systems, data or services connected to Starion. We will discuss any findings with you after the audit and agree on the necessary steps to address risks and strengthen your cybersecurity posture.

If non-compliance is identified, you may be required to implement a formal remediation plan within agreed timelines. Failure to remediate may result in suspension or termination of services, formal review of your cybersecurity practices, notification to regulatory authorities under NIS2 obligations, or financial penalties as defined in contractual agreements.

External Providers are expected to offer open, transparen, and complete collaboration during audits, so that assessments can be conducted efficiently and any recommendations swiftly agreed upon and implemented to ensure the ongoing protection of Starion's systems and data.

9 Contract termination and offboarding

To ensure secure disengagement and protect Starion's systems and data, all External Providers must follow these requirements upon contract termination or service offboarding:

1. **Access revocation:** All credentials, user accounts, API keys and system access rights must be revoked immediately upon contract end or termination notice. This includes access to Starion networks, applications, data repositories and any integrated systems.

2. **Data handling:** All Starion data in the provider's possession must be either securely returned with proper documentation or permanently destroyed in accordance with contractual obligations and applicable data protection laws. Written confirmation of data return or destruction must be provided.
3. **Final cybersecurity review:** A final cybersecurity compliance check must be completed before disengagement. This may include reviewing offboarding procedures, verifying access revocation, confirming data handling actions and assessing any residual risks or obligations.

Starion reserves the right to conduct or request this review and may require supporting documentation or evidence from the provider.

External Providers are expected to fully support Starion during contract termination and offboarding, and taking the necessary steps and providing the necessary confirmation to ensure that cybersecurity of systems and data is managed.

10 What if you do not comply with this standard?

We have specifically designed this External Provider Cybersecurity Standard to be adaptable to your business operations, while ensuring Starion can maintain confidence in how you protect our systems, data and services. Cybersecurity is a critical matter and failure to comply with this Standard can have serious consequences. If you cannot comply with this External Provider Standard and you perform services for Starion to which this External Provider Standard applies, it is your responsibility to notify Starion. We commit to work with you to understand how compliance can be achieved in a way that meets cybersecurity requirements.

If Starion identifies that an External Provider has not complied with this Cybersecurity Standard, we may require a rectification plan to be implemented at the provider's expense or terminate our contractual relationship for cause.

Starion commits to engaging proportionately and constructively with providers regarding this Standard and any breaches that may occur.