Policies

IONX Supplier Security Policy

Table of Contents

1. Purpose

This policy outlines specific security, privacy, and governance requirements for vendors and suppliers providing services, products, or support to our organization. It ensures adherence to robust cybersecurity, privacy standards, and supply chain risk management practices, reflecting industry best practices and regulatory mandates.

2. Scope

Applicable to all vendors, suppliers, contractors, and third-party service providers involved with telecommunications infrastructure, data, systems, software, and associated services for IONX, whether based in or providing services within the US and the UK.

3. Supply Chain Risk Management

Risk Assessment and Mitigation:

- Vendors must perform annual comprehensive supply chain risk assessments, focusing on cybersecurity risks, infrastructure vulnerabilities, network resilience, and potential business impacts.
- Critical vendors must maintain detailed incident response and business continuity plans, updated continuously, demonstrating strategies to mitigate identified risks.

Regular Auditing and Monitoring:

- Security audits and compliance evaluations must be performed at least annually or when significant changes occur in technology, service provision, or contractual agreements.
- Audit reports, specific to telecommunications infrastructure, must be delivered within 30 days post-audit.

4. Information Security Requirements

- Compliance with frameworks such as NIST Cybersecurity Framework, ISO 27001, ETSI EN 303645, IEC 62443, and regulations like Ofcom's UK Telecom Security Act and FCC guidelines.
- Annual penetration testing and vulnerability assessments must be conducted, with full documentation provided to our organization upon request.

Secure Product Lifecycle:

- Vendors must incorporate secure development lifecycles (SDL) ensuring verifiable security and privacy controls during development, manufacturing, and testing.
- Assurance that products, software, and services are free from malicious components including malware, viruses, Trojan horses, or backdoors.

Incident Management:

- Immediate reporting (within 24 hours) of security incidents affecting provided services and/or assets.
- Provide comprehensive incident reports detailing root causes, impacts, and corrective measures.

5. Data Privacy and Governance

Data Handling Compliance:

- Compliance with GDPR (UK), CCPA, CPRA (US), and other relevant telecommunications-specific privacy regulations.
- Strong encryption required for sensitive and personal data both in transit and at rest.

Access and Authorization:

- Access controls must adhere strictly to the principle of least privilege, verified by periodic reviews.

Data Retention and Disposal:

- Defined protocols for secure retention, timely disposal, and verifiable destruction of data post-use or contract completion.

6. Continuous Security and Maintenance

- Products, software, and services must undergo ongoing hardening by disabling unnecessary services and features.
- Vendors must provide regular security patches and updates promptly.
- Escrow arrangements for critical designs, source codes, and cryptographic materials may be required to ensure continuity of support.

7. Training, Awareness, and Documentation

- Regular, specialized security and privacy training required for vendor employees.
- Vendors must maintain detailed documentation of security training, available upon request.

8. Compliance and Enforcement

- A designated security and privacy contact person must be provided to oversee policy adherence.
- Non-compliance may result in contract reviews, mandatory remediation, and potential termination of agreements.

9. Policy Review and Updates

- Annual reviews or updates as necessary due to technological advancements, regulatory changes, or operational adjustments.
- Vendors will receive explicit and timely notifications of any policy amendments.

10. Authorization

This policy is approved and enforced by the IONX Security Council.

Effective Date: July 1, 2025
Policy Owner: Senior Director Information Security
Next Scheduled Review: June 30, 2026