

(Cyber)security annex for procurement

Aviation in (cyber)safe hands, including the supply chain

Contents

Contents	2
Introduction 4	
1.1 Scope	4
1.2 Hierarchy	4
Article 1 Definitions and references 5	
Definitions (Cyber)Security Annex for Procurement LVNL	5
Definitions (Cyber)security Annex	5
Article 2 Supplier Risk profile 7	
Distinction of Risk Profiles	7
Risk Profile: Normal	7
Risk Profile: Elevated	7
Validity of the Agreement	7
Article 3 Governance 8	
Information Security Organization	8
Information Security Policy	8
Information Security Risk Management	8
Annual Information Security Alignment	8
Duty of Care of the Counterparty	8
Article 4 Access control 9	
Access Management and User Rights	9
Article 5 Identities and Authentication 10	
Identity Management	10
Single Sign-On	10
Passwords	10
Multi-Factor Authentication (MFA)	10
Modification of Authentication Data	10
Deviation from Prescribed Authentication Measures	11
Article 6 Endpoint, Network and Application Security 12	
Endpoint Security	12
Network Security	12
Application and Software Security	12

Secure Configurations	12
Article 7 Cryptography and Key Management	13
Cryptography	13
Key Management	13
Article 8 Vulnerability Management	14
Identification of Vulnerabilities	14
Remediation of Vulnerabilities	14
Report on Technical Vulnerability Management	14
Article 9 Incident Reporting	15
Incident Reporting	15
Incident Reporting Contact Details	15
Cooperation in Incident Investigations	15
Article 10 continuity	16
Back-up and Recovery Procedures	16
Service Continuity	16
Article 11 Personnel Security and Subcontractor Management	17
Screening	17
Disciplinary Procedures	17
Subcontracting	17
Article 12 Audit, (Security) Testing and Compliance Monitoring	18
Security Audits, Risk Assessments and Penetration Tests	18
Article 13 Support in Compliance with Regulatory requirements	19
Support in Complying with Legal Obligations	19

Introduction

Suppliers play a critical role in LVNL's (primary) business processes and are therefore essential to safeguarding our digital resilience. To maintain continuous control over cyber risks and to ensure secure collaboration, LVNL applies specific terms and requirements relating to cybersecurity. In the context of any engagement with LVNL, suppliers are required to comply with these conditions. To ensure enforceability, this (Cyber)security annex forms an integral part of the contractual agreements. Suppliers are obliged to adhere to the defined security standards, including compliance with applicable laws and regulations, implementation of appropriate security measures, and the timely reporting of information security incidents.

1.1 Scope

The (Cyber)security Annex to the General Terms and Conditions of Procurement applies to the following types of Deliverables:

- **Software**, referring to off-the-shelf software and/or custom-developed software provided by the supplier;
- **Hardware**, including any embedded software and/or firmware;
- **XaaS/Cloud services** (for example, SaaS, IaaS, PaaS, etc.); and
- **Professional services** for the provision of installation, training, integration, maintenance, and/or consultancy services.

1.2 Hierarchy

This (Cyber) Security Annex forms an integral part of the Agreement between LVNL and the Supplier and, where applicable, is established through acceptance of the LVNL General Terms and Conditions of Procurement and/or by execution of the Agreement.

Article 1 Definitions and references

Definitions (Cyber)Security Annex for Procurement LVNL

For general definitions, Article 1 of the LVNL General Procurement Terms and Conditions shall prevail.

- 1.1. **Article:** an article as referred to in these General Terms and Conditions of Procurement;
- 1.2. **Services:** the services to be performed and/or work to be carried out by the Counterparty for the benefit of LVNL, on the basis of an Agreement;
- 1.3. **LVNL:** Luchtverkeersleiding Nederland, the public law legal entity established under the Aviation Act of 18 June 1992 (Bulletin of Acts and Decrees 1992, 368), having its registered office at (1117 CV) Schiphol, Stationsplein Zuid-West 1001;
- 1.4. **Deliverables:** the goods to be supplied by the Counterparty to LVNL on the basis of an Agreement;
- 1.5. **Additional Work:** additional goods to be supplied or additional services to be performed or work to be carried out;
- 1.6. **Quotation(s):** an offer within the meaning of the Dutch Civil Code;
- 1.7. **Request for Quotation (RFQ):** a single or multiple requests issued by LVNL for the performance of Services;
- 1.8. **Agreement:** any agreement concluded between LVNL and the Counterparty, by whatever name, relating to the performance of Services by or on behalf of the Counterparty;
- 1.9. **Party(ies):** LVNL and/or the Counterparty;
- 1.10. **Personnel:** employees and other staff, as well as third parties/auxiliaries engaged by the Counterparty in the performance of the Agreement;
- 1.11. **Performance:** the Deliverables and/or Services (to be provided);
- 1.12. **Supplier:** the natural or legal person who is the contractual counterparty of LVNL under the Agreement.

Definitions (Cyber)security Annex

- 1.13. **(Cyber) Security Annex:** this Annex relating to the Cyber Security Requirements and Cyber Security Measures.
- 1.14. **Cyber Security Requirements:** the specific requirements (controls and measures) in the field of information security as set out in this (Cyber) Security Annex, which the Counterparty is required to comply with.
- 1.15. **Cyber Security Controls:** the organizational and technical (security) measures in the field of information security that the Counterparty implements and maintains in order to comply with (i) applicable laws and regulations, (ii) the Cyber Security Requirements, and (iii) the Agreement. In addition, the Supplier shall apply, where relevant and proportionate to the performance of the Agreement, generally accepted industry best practices applicable to the sector in which the Counterparty operates (such as the ISO/IEC 27000 series, IEC 62443, ISAE 3402, SOC 2, ISF, and NIST).
- 1.16. **Cyber Security Risks:** risks relating to (the safeguarding of) the confidentiality, integrity, and availability of information, assets, systems of, and services provided to LVNL.
- 1.17. **Equipment:** the hardware to be delivered and/or deployed under the Agreement, including in any case computers, servers, network components, peripherals, and other physical ICT facilities, including the associated software, firmware, documentation, accessories, and appurtenances, insofar as these are necessary for their operation, implementation, or use.
- 1.18. **Software:** all software, in any form and on any medium, including associated updates, patches, configurations, interfaces, documentation, and other components that are delivered, made available, implemented, or maintained by the Counterparty under the Agreement.

- 1.19. **Hardware:** all physical ICT components and electronic facilities, including the associated firmware, parts, documentation, and accessories, that are delivered, made available, or deployed by the Counterparty under the Agreement.
- 1.20. Internet-facing Systems: systems that are publicly accessible via the internet and reachable through one or more ports.
- 1.21. **(Information) Security Incident:** a single unwanted or unexpected (information) security event, or a series of related events, that can reasonably be expected to have a material impact on business operations and constitutes a threat to information security.

Article 2 Supplier Risk profile

Distinction of Risk Profiles

Not all suppliers, products, and collaborations are equivalent from the perspective of operational risk. To make this distinction, LVNL conducts a risk analysis for each prospective Agreement, resulting in a supplier risk profile. The following aspects set out the requirements for determining the risk profiles and the (Cyber)security requirements associated with the different risk profiles.

- 2.1 The Counterparty is obliged to cooperate with (and, if requested by LVNL, provide information for the purpose of) a risk analysis to be carried out by LVNL, on the basis of which LVNL determines the risk profile of the Deliverables.
- 2.2 LVNL applies two risk profiles for collaborations with the Counterparty: Normal and Elevated.

Risk Profile: Normal

- 2.3. For a “Normal” risk profile, LVNL verifies whether the Deliverables to be procured comply with the Cyber Security Requirements. As substantiation, the Supplier shall, at LVNL’s request, provide at least: (1) a completed and signed self-certification (CYRA) and/or (2) a valid ISO/IEC 27001 certificate, or (3) a certificate/report accepted by LVNL in writing as equivalent. The scope thereof shall cover at least the service and/or product and the supporting processes relevant to the Deliverables. Any deficiencies identified by LVNL shall be discussed with the Supplier prior to the commencement of the Services and remedied by the Supplier within a period to be determined by LVNL (following consultation), unless LVNL accepts such deficiencies in writing as a risk.

Risk Profile: Elevated

- 2.4. For an “Elevated” risk profile, LVNL verifies whether the Deliverables to be procured comply with the Cyber Security Requirements. The Supplier shall, throughout the term of the Agreement, hold valid certifications applicable to the Deliverables and, where appropriate, audit reports from an independent third party, being (1) an ISO/IEC 27001 certificate or (2) a certificate/report accepted by LVNL in writing as equivalent. The Counterparty shall provide LVNL with a copy of the applicable certificates and the corresponding (audit) reports. The scope thereof shall cover at least the service and/or product and the supporting processes relevant to the Deliverables. Any deficiencies identified by LVNL shall be discussed with the Supplier prior to the commencement of the Services and remedied by the Supplier within a period to be determined by LVNL (following consultation), unless LVNL accepts such deficiencies in writing as a risk.

Validity of the Agreement

- 2.5. If the Counterparty fails to comply with a timeline established and confirmed in writing by LVNL for remedying deficiencies, or if it is unable to provide the required certifications and/or audit reports in a timely manner, or if such certifications and/or audit reports are no longer valid, or are suspended or withdrawn, LVNL shall be entitled to terminate the Agreement in whole or in part after written notice of default and the expiry of a reasonable cure period without remedy. LVNL shall be entitled to terminate the Agreement in whole or in part with immediate effect, without judicial intervention, if (a) the deficiency is by its nature not remediable, or (b) immediate termination is reasonably necessary to limit (cyber) security, continuity, or compliance risks. In the event of termination pursuant to this Article, the Supplier shall not be entitled to any compensation or damages in connection with such termination. The Supplier shall demonstrate at least annually, and additionally upon LVNL’s request, that the certifications and/or audit reports referred to in the applicable risk profile remain valid.

Article 3 Governance

Information Security Organization

- 3.1. The Counterparty is obliged, if requested by LVNL, to provide information regarding its own information security organization.
- 3.2. The Counterparty shall appoint both a contact person for security-related matters and a contact person at senior management level, or a key account manager, for handling escalations. Contact details must be kept up to date, and any changes thereto must be communicated to LVNL without delay.

Information Security Policy

- 3.3. The Counterparty is obliged to maintain an information security policy that is in accordance with the requirements and principles of the ISO/IEC 27001 standard, or a comparable, industry-recognized standard. This policy must be kept up to date and provided to LVNL for inspection upon request.
- 3.4. If the Counterparty holds one or more relevant security certification(s), it is obliged to provide these to LVNL upon first request. The Counterparty shall inform LVNL in writing of any change in the scope of its certification(s), as well as any extensions or renewals thereof, within 30 days after such change has occurred. In the event of suspension, withdrawal, or otherwise loss of a valid certification, the Counterparty shall notify LVNL without delay, and no later than within 7 days.
- 3.5. If the Counterparty has been selected by LVNL on the basis of a certification (for example ISO/IEC 27001), the Supplier shall maintain such certification throughout the entire duration of its contractual obligations.

Information Security Risk Management

- 3.6. The Supplier shall apply a systematic process for risk management to control Cyber Security Risks that may affect the confidentiality, integrity, and availability of information and services. This process shall be integrated into business operations and be continuously maintained and improved.

Annual Information Security Alignment

- 3.7. Annually, at the request of one or both Parties, the Counterparty and LVNL shall organize a meeting to discuss security aspects (for example developments and planned activities that may affect security). Either Party may request an extraordinary security meeting, which shall be accepted by the other Party if the situation requires a joint analysis or an immediate decision (for example in the event of a serious incident or a significant development in threats).

Duty of Care of the Counterparty

- 3.8. The fact that LVNL prescribes or approves specific security measures does not release the Counterparty from its own duty of care with respect to information security. The Counterparty shall at all times remain fully responsible for implementing and maintaining all reasonable and appropriate technical and organizational measures to protect the information, systems, and data under its control or responsibility. This obligation extends to compliance with generally accepted security standards and best practices, irrespective of any instructions or approvals provided by LVNL.

Article 4 Access control

Access Management and User Rights

- 4.1. The Supplier shall apply the principle of “least privilege” when granting access rights, whereby access is granted only insofar as necessary for the performance of activities within the user’s role and in the context of the Agreement.
- 4.2. The Counterparty shall maintain an up-to-date register of all Personnel and engaged third parties involved in the Services who have access to LVNL information, assets, and systems.
- 4.3. During the provision of the Services, the Counterparty shall periodically review the access rights recorded in the register referred to in the previous Article. For privileged accounts (e.g., management, administrative), the Counterparty shall perform such review at least every 90 days. For other accounts, the Counterparty shall perform such review at least annually.
- 4.4. LVNL is entitled to temporarily block or deactivate one or more accounts of the Counterparty and/or users authorized by or on behalf of the Counterparty, as well as to temporarily suspend the Counterparty’s access to (parts of) LVNL’s ICT environments, systems, applications and/or data, if: (1) a (Information) Security Incident or data breach has occurred, or (2) there is a reasonable suspicion of a (attempted) (Information) Security Incident, data breach, unauthorized access, or other breach(es) of the confidentiality, integrity, or availability of LVNL’s systems or data.
- 4.5. LVNL shall limit any measure as referred to in Clause 4.4 to what is reasonably necessary to investigate the (suspected) incident, limit its impact, and prevent further damage or breaches, and shall inform the Counterparty as soon as possible of the reason for and expected duration of the suspension, unless overriding security or law enforcement interests prevent this.
- 4.6. The Counterparty shall ensure that each user account is personal in nature. This includes accounts issued to an individual user and excludes accounts issued to a group or department, thereby ensuring traceability of actions.
- 4.7. Group accounts are not permitted, unless LVNL has explicitly granted permission to the Counterparty.

Article 5 Identities and Authentication

Identity Management

- 5.1. The Counterparty shall support, for the products and/or Services delivered under the Agreement, integration with LVNL's Identity & Access Management (IAM) environment. Where applicable, the Counterparty shall additionally support automated provisioning and deprovisioning of LVNL users and their authorizations through commonly used standards such as SCIM.
- 5.2. If the Counterparty is unable (or no longer able) to comply with LVNL's Identity & Access Management procedures, the Parties shall jointly agree on an alternative procedure for account management, after which the Counterparty shall submit the proposed alternative procedure to LVNL for approval. Following written approval by LVNL, the Supplier shall ensure that it has and maintains formal procedures for the timely creation, modification, and deletion of (administrative) accounts, where "timely" shall mean within 92 calendar days.

Single Sign-On

- 5.3. To the extent that the Counterparty provides a service or application for use by LVNL users, support for Single Sign-On (SSO) via the Identity Provider designated by LVNL is required, using commonly accepted federated standards (such as SAML 2.0 and/or OpenID Connect).

Passwords

- 5.4. The Supplier shall ensure that passwords for all accounts, including those of administrators and users engaged by the Supplier, are stored using a secure, up-to-date one-way hash mechanism, including a unique salt per user.
- 5.5. The Counterparty shall ensure that passwords for user accounts with access to LVNL data and systems are strong, that password requirements are automatically enforced, and that they comply with guidelines and best practices established by the National Institute of Standards and Technology (NIST). Passwords shall be changed in the event of a suspected breach or an (Information) Security Incident. The use of a password vault is recommended to further secure access.
- 5.6. Passwords for administrative accounts used by the Supplier shall be at least 16 characters in length. No additional complexity requirements apply to a passphrase, except that it must not consist of 16 consecutive or identical characters, nor of contextually easily derivable elements (such as slogans, addresses, place names, football clubs, etc.). These passwords must be changed in the event of a suspected breach or an (Information) Security Incident. The Supplier should preferably use a Privileged Access Management (PAM) system to manage and monitor access to administrative accounts.

Multi-Factor Authentication (MFA)

- 5.7. The Supplier shall ensure that strong authentication (specifically MFA) is used for: (1) accounts of the Counterparty with elevated (administrative) privileges, (2) access to systems that process sensitive data, and (3) access to facilities accessible via the internet.

Modification of Authentication Data

- 5.8. All authentication data, including cryptographic keys, in Software, Hardware, and Equipment or Services to be provided by the Supplier must be modifiable by LVNL and shall be protected in accordance with the current state of the art. If for certain authentication data cannot be modified by LVNL, the Supplier shall provide LVNL with an overview thereof, including the purposes for which such data are used.

Deviation from Prescribed Authentication Measures

- 5.9. If the Supplier wishes to apply alternative methods and measures to protect accounts that replace the use of passwords, such measures must be approved by LVNL in advance.

Article 6 Endpoint, Network and Application Security

Endpoint Security

- 6.1. The Counterparty shall implement up-to-date anti-malware solutions on all endpoints used for the provision of the Services (including servers, workstations, and mobile devices). Malware signatures shall be updated daily. The Supplier shall collect the necessary logging and actively monitor for suspicious activities. If anomalies are detected, the Supplier shall take appropriate response and remediation measures.
- 6.2. To the extent that the Supplier uses software, tooling, and/or configurations provided by LVNL (including, but not limited to, VPN clients), LVNL is entitled to technically verify the security status of the relevant endpoints, solely insofar as this is necessary to verify compliance with LVNL's security requirements.

Network Security

- 6.3. The Supplier shall implement all controls in accordance with the most recent industry best practices necessary to protect the availability, confidentiality, and integrity of data transmitted via physical or wireless networks, as well as connected systems and applications. Appropriate controls shall include, at a minimum, network segmentation, the use of firewalls, intrusion detection/prevention systems (IDS/IPS), and centralized monitoring.

Application and Software Security

- 6.4. To the extent that the Supplier develops, modifies, configures, and/or delivers Software under the Agreement, the Counterparty shall demonstrably test such Software in accordance with generally accepted industry standards for application security, such as the OWASP Application Security Verification Standard (OWASP ASVS), or a comparable security standard. In such cases, the Supplier shall ensure an adequate process for identifying, assessing, remediating, and managing vulnerabilities in the Software, including in any event the timely provision and implementation (or causing the implementation) of security updates and patches that remediate critical or high vulnerabilities.

Secure Configurations

- 6.5. The Counterparty shall perform system and software hardening as a baseline in accordance with CIS Benchmark hardening standards (and, where these are not available, in accordance with the supplier's hardening standards) in order to ensure a secure configuration.

Article 7 Cryptography and Key Management

Cryptography

- 7.1. The Supplier shall use cryptographic operations to secure the data it processes. It shall apply encryption to data transmitted over networks, to data stored on (portable) Equipment, and on removable media, such as USB sticks, and in other situations where data is vulnerable to access by unauthorized persons.
- 7.2. Encryption shall be applied using algorithms, protocol versions, and key strengths that are included in, or aligned with, the recommendations applicable at that time of BSI, NCSC-NL, ENISA, and/or NIST.
- 7.3. The use of weak, outdated, or otherwise insecure cryptographic algorithms, protocols, and configurations is not permitted.
- 7.4. For Services or systems accessible via the internet, self-signed certificates shall not be used unless LVNL has granted prior written approval for such use. Public certificates must be issued by a trusted certification authority.

Key Management

- 7.5. The Supplier shall ensure proper key management, which shall in any event include the secure generation, distribution, storage, rotation, revocation, replacement, and destruction of cryptographic keys, as well as restriction of access thereto on the basis of need-to-know and least privilege. Keys and associated secret values shall be protected in such a way that unauthorized access, modification, disclosure, or misuse is reasonably prevented.

Article 8 Vulnerability Management

Identification of Vulnerabilities

- 8.1. The Supplier shall continuously monitor relevant security advisories, vulnerability notifications, and patches, and shall inform LVNL without delay of vulnerabilities that are or may be relevant to the availability, integrity, or confidentiality of the environment or of the data processed by the Supplier.
- 8.2. If critical vulnerabilities are identified, the Supplier shall notify LVNL thereof immediately, and additional measures shall be taken in accordance with Table 1 to remediate such vulnerabilities.

Remediation of Vulnerabilities

- 8.3. The Supplier shall ensure demonstrable and adequate patch management and vulnerability management for all Software, Hardware, and other ICT components delivered or used under the Agreement. The Supplier shall identify vulnerabilities, assess their severity, and take appropriate measures within the following timeframes:

Vulnerability category	CVSS 4.0	Internet facing systems	Non-internet facing systems
Critical	A score between 9.0 and 10.0	No later than 48 hours	1 week
High	A score between 7.0 and 8.9	1 week	1 month
Medium	A score between 4.0 and 6.9	1 month	2 months
Low	A score between 0.1 and 3.9	Best effort	Best effort

Table 1 – Overview of remediation periods by vulnerability category and system category

- 8.4. If remediation within the aforementioned timeframes is not reasonably possible, the Supplier shall implement mitigating measures without delay and shall coordinate the further approach with LVNL in writing.

Report on Technical Vulnerability Management

- 8.5. The Supplier shall prepare a periodic internal report (monthly) on the status of patching, hardening, and the handling of relevant vulnerabilities, and shall share this report with LVNL upon request.

Article 9 Incident Reporting

Incident Reporting

- 9.1. If the Supplier has identified an (Information) Security Incident relating to information, assets, and systems (of LVNL and/or the Supplier) or procured Services under the Agreement, the Supplier shall report this without delay, but in any event within 24 hours after becoming aware of it, to LVNL's contact point set out below. The Supplier shall also inform LVNL's regular contact person or contract manager.
- 9.2. LVNL is entitled to unilaterally change the contact details of this contact point during the term of the Agreement and shall inform the Supplier accordingly. When reporting incidents, the Supplier shall at all times use the most current contact details communicated by LVNL.

Incident Reporting Contact Details

Telephone number: **[to be completed by LVNL upon contract conclusion]**
Email address: **[to be completed by LVNL upon contract conclusion]**

- 9.3. The report shall include at least, insofar as available at that time: the nature of the incident, the time of discovery, the systems or data affected or suspected to be affected, the possible impact, measures already taken, and the contact details of the Suppliers incident response contact point. The Supplier shall then provide periodic updates to LVNL until the incident has been resolved and its consequences have been remedied.

Cooperation in Incident Investigations

- 9.4. The Supplier shall fully cooperate with investigations, forensic investigations, remediation measures, and, where applicable, notifications to regulators, affected persons, or other competent authorities. After the incident has been handled, the Supplier shall provide LVNL with a written incident report, including root cause analysis, implemented controls, lessons learned, and improvement measures to prevent recurrence.

Article 10 continuity

Back-up and Recovery Procedures

- 10.1. The Supplier shall ensure appropriate and demonstrable measures in the area of continuity, backup, and disaster recovery for the services and/or systems relevant to LVNL's environment. The Supplier shall ensure that data and configurations are backed up in an adequate and secure manner, that recovery procedures are available and up to date, and that these arrangements are tested periodically.
- 10.2. The Supplier shall carry out disaster recovery tests on a regular basis and shall provide the results thereof to LVNL upon request. If the tests reveal deficiencies, the Supplier shall take corrective measures without delay and report on the progress of the follow-up.

Service Continuity

- 10.3. The Supplier shall ensure sufficient staffing with qualified personnel and shall guarantee that the deployment of personnel, knowledge, and resources is adequate to support the continuity of the Services. The Supplier shall furthermore provide reasonable cooperation with LVNL's continuity planning, insofar as this relates to the services, systems, or facilities to be provided or provided by the Supplier.

Article 11 Personnel Security and Subcontractor Management

Screening

- 11.1. The Supplier shall ensure appropriate security screenings and thorough assessments (screening) for all personnel who have direct or indirect access to sensitive systems, data, or services, insofar as legally permitted and proportionate in the context of the Agreement. Personnel with such access shall undergo role-based security training and an awareness program prior to being granted access rights and periodically thereafter; the training shall be tailored to risk, role and responsibilities.
- 11.2. Where the Supplier or its personnel use LVNL systems, LVNL may require that the relevant persons hold a Certificate of Conduct (Verklaring Omtrent het Gedrag, VOG), insofar as this is required under applicable law or LVNL policy.
- 11.3. Where the Supplier or its personnel require physical access to spaces designated by LVNL as vital or secure, LVNL may additionally require those persons to hold a Security Clearance (Verklaring van Geen Bezwaar, VGB), insofar as this is required under applicable law or LVNL policy.

Disciplinary Procedures

- 11.4. The Supplier shall maintain a clear disciplinary regime that permits immediate action where there is suspicion of intentional or grossly negligent breach of information security obligations, including suspension of work and immediate blocking or revocation of access rights. The Supplier shall ensure that access rights are changed or revoked without delay when required due to a change of role, termination of engagement, or security reasons.

Subcontracting

- 11.5. Where the Supplier engages subcontractors or sub-suppliers involved in the performance of the Agreement, the Supplier shall identify those parties to LVNL in writing in advance, to the extent relevant. The Supplier shall contractually bind subcontractors and sub-suppliers to at least equivalent information security requirements as those set out in this (Cyber) Security Annex. Where subcontractors or sub-suppliers have access to sensitive Deliverables, systems, or data, the Supplier shall, insofar as legally permitted and proportionate, subject them to appropriate security screening and safeguards.

Article 12 Audit, (Security) Testing and Compliance Monitoring

Security Audits, Risk Assessments and Penetration Tests

- 12.1. The Supplier acknowledges that LVNL has the right to conduct or have conducted by a third party appointed by LVNL, security audits, risk assessments and penetration tests, no more than once per year. The Supplier shall fully cooperate in this regard, including by providing access to relevant systems, documentation and personnel, subject to applicable legal and contractual restrictions.
- 12.2. Any identified security deficiencies shall be remedied by the Supplier within the agreed timeframes. If the Supplier fails to remedy such deficiencies in a timely or adequate manner, LVNL shall retain all rights and remedies available to it under applicable law and contract.

Article 13 Support in Compliance with Regulatory requirements

Support in Complying with Legal Obligations

- 13.1. The Supplier undertakes to support LVNL in complying with its legal and supervisory obligations arising from the NIS2 Directive, as well as any applicable national and international sector-specific regulations applicable to LVNL.
- 13.2. Upon request and within a reasonable period, the Supplier shall provide appropriate information, documentation, and supporting data, insofar as this is legally permitted and reasonably required. The Supplier shall also provide all necessary information legally permitted to support notifications to, or consultations with, the competent supervisory authorities, including information regarding (Information) Security Incidents, vulnerabilities, mitigation measures, and the security posture of the Services, systems, and Deliverables to be provided or provided by the Supplier. If legal or contractual restrictions prevent the disclosure of complete information, the Supplier shall immediately provide a reasoned explanation. In such case, the Supplier shall proactively propose alternative solutions (such as anonymization) in order to ensure that the necessary transparency for LVNL and the supervisory authorities is nevertheless maintained.

