Security Annex

Introduction
SNBV acknowledges that suppliers play a crucial role in safeguarding the digital security of our organization. To manage the risks associated with cyber threats and ensure secure collaboration, SNBV applies specific conditions and requirements that all suppliers must comply with. These guidelines form an integral part of our contractual agreements. Suppliers are obliged to adhere to the established security standards, including compliance with relevant laws and regulations, implementation of appropriate technical and organizational measures, and timely reporting of security incidents.

The Security Annex applies to the (information) security of (i) the supply of goods, documentation, hardware or software, and (ii) the provision or performance of services, including SaaS or maintenance, as assigned to [Supplier] under the Agreement, hereinafter referred to as the "Deliveries".

This Security Annex constitutes an integral part of the Agreement between SNBV and the Supplier and is established through acceptance of the General Purchase Conditions (IT & Systems), hereinafter referred to as GPC, and/or by signing the Agreement.

If SNBV and the Supplier so desire, they may agree upon a customized Security Annex and include it as an appendix to the Agreement or to a data processing agreement. In such case, the customized Security Annex shall replace this Security Annex.

This Security Annex remains applicable for as long as the Supplier provides the Deliveries to SNBV in accordance with the Agreement and terminates when the Agreement ends, without prejudice to obligations that by their nature survive the Agreement (such as confidentiality and secure return/destruction).

The applicable version of this Security Annex is the version that is available online at the time of acceptance of the GPC or the conclusion of the Agreement. All previous versions remain digitally accessible to determine which version applied to a specific legal relationship.

1. Definitions

1.1. Capitalised terms used but not defined in this Cyber Security Annex have the meanings assigned in the Agreement and the General Purchase Conditions (IT & Systems). In addition, the terms below have the following meanings:
1.2. Security Annex: This Annex governs the Cybersecurity Requirements and Cybersecurity Measures.
1.3. Cyber Security Requirements: the specific, verifiable requirements (controls/requirements) related to information security that are included in this Security Annex and that the Supplier must comply with.
1.4. Cyber Security Measures: the information security measures that (i) stem from laws and regulations as well as industry best practices (e.g. ISO/IEC 27000-serie, IEC 62443, ISAE3402, ISF and NIST) for the sector in which the Supplier operates, insofar as relevant to the execution of the Agreement and the assignment to be performed by the Supplier, and/or (ii) arise from Cyber Security Requirements applied by SNBV to the organisation of the Supplier and the products and/or services provided by it, and/or (iii) arise from the Agreement.
1.5. Cyber Security Risks: risks regarding (safeguarding) the confidentiality, integrity and availability of information, business assets, systems of and the service provision to SNBV.
1.6. Self-Certification (CYRA): Mapping the level of information security through an online self-assessment, with the option for independent certification (https://hetccv.nl/keurmerken/cybersecurity/cyra/)

2. Supplier Risk Profile

2.1. The Supplier shall be obliged to cooperate with (and, if requested by SNBV, provide information for) a risk assessment to be carried out by SNBV, on the basis of which SNBV shall determine the risk profile of the Deliveries. SNBV applies three (3) risk profiles:

2.2. **Classification Low:** For a 'Low' risk profile, SNBV shall verify whether the Delivery to be procured complies with the Cyber Security Requirements. As supporting evidence, the Supplier shall, upon SNBV's request, provide at least (i) a completed and duly signed self-certification (CYRA) and/or (ii) a valid ISO 27001 certificate (if available). Any deficiencies identified by SNBV shall be discussed with the Supplier prior to commencement of the services and shall be remedied by the Supplier within a period to be determined by SNBV (following consultation), unless SNBV accepts such deficiencies in writing as an acceptable risk.

2.3. **Classification Medium:** For a 'Medium' risk profile, SNBV shall verify whether the Delivery to be procured complies with the Cyber Security Requirements. Throughout the term of the Agreement, the Supplier shall hold valid certifications applicable to the Delivery(ies) and, where appropriate, audit reports issued by an independent third party, being (i) an ISO/IEC 27001 certificate or (ii) a SOC 2 report (Type II if required by SNBV), or alternatively a certificate/report expressly accepted in writing by SNBV as equivalent. Where the Delivery(ies) include industrial automation and control systems (IACS), the Supplier shall additionally hold demonstrable implementation/certification in accordance with IEC 62443 (relevant parts), as specified by SNBV. The Supplier shall provide SNBV with a copy of the applicable certificates/reports. The scope thereof shall cover at least the service/product components and supporting processes relevant to the Delivery(ies). Any deficiencies identified by SNBV shall be discussed with the Supplier prior to commencement of the services and shall be remedied by the Supplier within a period to be determined by SNBV (following consultation), unless SNBV accepts such deficiencies in writing as an acceptable risk.

2.4. **Classification High:** For a 'High' risk profile, SNBV shall verify whether the Delivery to be procured complies with the Cyber Security Requirements. Throughout the term of the Agreement, the Supplier shall hold valid certifications and/or audit reports applicable to the Delivery(ies), issued by an independent third party, consisting of (i) an ISO/IEC 27001 certificate and, in addition, (ii) a SOC 2 Type II report or an ISAE 3402 report, or alternatively an assurance report expressly accepted in writing by SNBV as equivalent. Where the Delivery(ies) include industrial automation and control systems (IACS), the Supplier shall additionally hold demonstrable implementation/certification in accordance with IEC 62443 (relevant parts), as specified by SNBV. The Supplier shall provide SNBV with a copy of the applicable certificates and the corresponding (audit) reports. The scope thereof shall cover at least the (online) service and/or product and the supporting processes relevant to the Delivery(ies). Any deficiencies identified by SNBV shall be discussed with the Supplier prior to commencement of the services and shall be remedied by the Supplier within a period to be determined by SNBV (following consultation), unless SNBV accepts such deficiencies in writing as an acceptable risk.

2.5. **Validity of the Agreement:**
If the Supplier fails to comply with a timeline established and confirmed in writing by SNBV for remedying deficiencies (i), or (ii) cannot provide the required certifications and/or audit reports in a timely manner, if such certifications or reports are no longer valid, or are suspended or revoked, SNBV shall be entitled to terminate the Agreement in whole or in part after issuing a written notice of default and allowing a reasonable period for remedy to lapse unused. SNBV 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 irreparable, or (b) immediate termination is reasonably necessary to mitigate (cyber)security, continuity, or compliance risks. In the event of termination under this article, the Supplier shall not be entitled to any compensation for damages resulting from such termination. The Supplier shall demonstrate at least annually, and additionally upon SNBV's request, that the certifications and/or audit reports specified in the applicable risk profile remain valid.

3. Responsibilities and compliance with Cyber Security Requirements

3.1. The Supplier is obliged to implement, comply with, evaluate and maintain the Cyber Security Measures at its own expense and risk, during the term of the Agreement, and to report on them to SNBV.

3.2. The Supplier shall take action to ensure that its staff and any third parties involved in executing the Agreement, such as subcontractors, suppliers, advisers and financiers, comply with Cyber Security Requirements and, for this purpose, the Supplier shall provide them with a copy of the Cyber Security Annex.

3.3. The Supplier shall periodically verify and evaluate whether its undertaking and the products and/or services provided by it under the Agreement comply with the obligations ensuing from this Cyber Security Annex. The Supplier shall immediately inform SNBV in writing in the event it is unable or no longer able or anticipates it will not be able to meet one or more obligations ensuing from this Cyber Security Annex

during the term of the Agreement. In that case, the Parties will discuss whether the Supplier can implement alternative Cyber Security Measures that are acceptable to SNBV.

3.4. At SNBV's request, the Supplier shall provide written reports demonstrating that the Supplier and any third parties engaged by it in executing the Agreement comply with the obligations under this Cyber Security Annex.

3.5. The Supplier is responsible for preventing and managing all Cyber Security Risks that occur, or may occur, in connection with the execution of the Agreement by the Supplier. The Supplier will deploy risk management in order to identify and mitigate Cyber Security Risks by implementing organisational and technical risk mitigation Cyber Security Measures and evaluating their operation.

3.6. If the Supplier identifies a Cyber Security Risk while executing the Agreement, the Supplier is required to report this to SNBV in writing within 7 calendar days of identifying the risk concerned. This report shall include at least the following information:

a. description of the cyber security risk;
b. the proposed control measures to prevent, eliminate, mitigate or transfer the risk;
c. the timeframe within which the measures referred to under b) will be implemented.

3.7. When requested to do so by SNBV, the Supplier shall support SNBV in complying with the obligations applicable to Royal Schiphol Group N.V. as a 'provider of an essential service' under the Cyberbeveiligingswet/NIS2 and the related Decree.

4. IT Service Management

4.1. The Supplier shall ensure that *industry best practices* around IT Service Management are implemented and maintained, as described in frameworks such as ITIL. These *industry best practices* are intended to ensure that the Supplier's IT services are managed and delivered effectively and efficiently, in line with SNBV's requirements and expectations.

5. Staff and Third Parties Engaged

5.1. The Supplier shall ensure that all staff and third parties engaged by it that are involved in executing the Agreement, upon commencement as well as during the term of the Agreement, receive training in the field of cyber security appropriate to their position and responsibilities when carrying out the work in connection with the Agreement. In order to be able to comply with this obligation, the Supplier shall in any case arrange a security awareness programme, training programmes and activities on the basis of prevailing industry best practices.

5.2. The Supplier shall ensure that, prior to commencement of the Agreement, a background check has been carried out for the members of staff and/or third parties engaged that are involved in executing the Agreement. These persons/organisations will only be given access to the information, business assets, systems and service provision of SNBV (that is/are relevant to the Agreement) in the case of a positive outcome of the background check. The background check must be performed in accordance with the applicable laws, regulations and ethical standards, while it must also be proportionate to the nature and scope of the access that the staff concerned and/or third parties engaged will have to SNBV's information, business assets, systems and services.

5.3. The Supplier shall ensure that during the term of the Agreement a formal disciplinary procedure shall apply to its legal relationship with staff and third parties engaged, which procedure shall provide for the consequences of non-compliance with Cyber Security Requirements by a member of staff or third party engaged. The disciplinary procedure shall be drafted in accordance with prevailing industry best practices. This procedure shall in any case provide for the Supplier's power to impose the immediate suspension and revocation of access rights and privileges relating to SNBV's information and systems where there is a suspicion that the aforementioned breach is the result of wilful intent or gross negligence. The Supplier is required to report such cases in writing to SNBV without delay.

6. Access control

6.1. The staff who are deployed and/or third parties that are engaged in executing the Agreement shall only have access to those parts of SNBV's information, business assets and systems as well as SNBV's service provision locations insofar as necessary to perform their tasks within the scope of their position and in connection with the Agreement (the principle of least privilege (PoLP)).

6.2. The Supplier shall ensure that each account is uniquely assigned to an individual user, and not to a group or department, to allow precise tracing of user actions at all times. Group accounts and functional accounts are not permitted, unless SNBV has given explicit consent to the Supplier for them.

6.3. The Supplier shall maintain a list of all the staff and third parties engaged that are involved in providing the services who have access to SNBV's information, business assets and systems. During the provision of

services, the Supplier shall check this list at least every 90 days to ensure that the principle of least privilege is being complied with and remaining/redundant accounts are deleted.

7. Risk analyses, technical risk assessments and audits

7.1. During the term of the Agreement, SNBV shall have the right to carry out, or arrange for independent third parties to carry out, risk analyses, technical risk assessments (including penetration tests) and audits of the service provision of the Supplier at its own expense. The Supplier is obliged to cooperate in these activities and to facilitate these risk analyses, technical risk assessments and audits, including by making relevant information security documents, standards, process descriptions, documentation and information available to SNBV in a timely and complete manner.

7.2. A risk analysis, technical risk assessment or audit as referred to in paragraph 1 above shall: (a) take place no more than once a year; and (b) result in the preparation of a confidential report. SNBV will provide the Supplier with a copy of the report. The Supplier shall implement, within the agreed time period, all the preventive and/or corrective actions further to the findings that were identified as a result of the aforementioned risk analyses, technical risk assessments and audits.

8. Network, Communication and Endpoint security

8.1. The Supplier shall put in place all control measures that are necessary to protect the availability, confidentiality and integrity of data transmitted via physical or wireless networks in accordance with the most recent industry best practices, as well as to protect connected systems and applications. Appropriate control measures include, but are not confined to, Firewalls, Proxies, Intrusion Detection Systems and Intrusion Prevention Systems, network segmentation and monitoring solutions.

8.2. The Supplier shall put in place all control measures that are necessary to protect all endpoints (e.g. servers, workstations and laptops) that are used for the provision of services against malware. In that connection, the Supplier shall install for the endpoint anti-malware management software, whose signatures are automatically updated at least once a day and continuously monitor it for suspicious activity.

8.3. The Supplier is required to use cryptographic processing to protect the data it processes. It shall apply encryption when transmitting data across networks, when storing data on portable and other devices and on removable media, such as USB sticks, and in other situations where data are vulnerable to access by unauthorised persons (such as data that can be accessed online). For this purpose, encryption will be implemented according to the latest standards and will be updated whenever it is determined that the existing standards no longer comply with the specified requirements.

a. Secure technologies such as the Advanced Encryption Standard (AES) technology with 256-bit or longer keys must be used for the storage of data. All keys used for this purpose must be managed in such a way that they are inaccessible to unauthorised persons and cannot be abused.

b. The Supplier will use secured connections when accessing websites and using applications and services, so that the network traffic between the client and the web server is safeguarded from unauthorised access or modification by third parties. The Supplier shall ensure that its websites, applications and services use certificates issued by a recognised public Certificate Authority (CA), such as DigiCert and VeriSign. The certificate must comply with the current requirements of the CA/Browser Forum Baseline Requirements for Contents of Publicly Trusted SSL/TLS Certificates. Self-signed certificates are not permitted.

9. Passwords

9.1. The Supplier shall ensure that the passwords of all accounts, of both administrators and users engaged by the Supplier, are stored using a secure, up to date one-way-hash mechanism (including unique salt).

9.2. The Supplier shall ensure that passwords for user accounts with access to SNBV data and systems are strong, are at least twelve characters long and consist of characters from at least three categories, such as upper-case letters, lower-case letters, numbers and special characters. These passwords must be replaced within a maximum period of 92 days or in the event of a suspected breach or security incident. For additional access security, measures such as multi-factor authentication (MFA) and a secure password vault are recommended.

9.3. The passwords for administration accounts that are used by the Supplier must be very strong, must be at least 15 characters long and must consist of characters from at least three categories, such as upper-case letters, lower-case letters, numbers and special characters. These passwords must be replaced within a maximum period of 180 days or in the event of a suspected breach or security incident. Preferably, the Supplier should use a Privileged Access Management (PAM) system to manage and monitor access to administration accounts.

9.4. The Supplier shall ensure that strong authentication (such as MFA) is used for (i) accounts with enhanced rights of the Supplier, (ii) access to systems processing sensitive data, and (iii) remote access via internet.

9.5. Prior approval must be obtained from SNBV in the event the Supplier wishes to implement alternative methods and measures to protect accounts in place of passwords.

10. Patching & hardening

10.1. The software used or supplied by the Supplier in executing the Agreement (OS, database, middleware and application software) shall feature all the known security patches issued by the Supplier, developer or programmer. These are applied or supplied in accordance with the table below when the patches are released:

Category	CVSS v3 Base score	Remediation time in case internet facing	Remediation time in case not internet facing
Low	0.0 - 3.9	Best effort	Best effort
Medium	4.0 - 6.9	1 month	2 months
High	7.0 - 8.9	2 weeks	1 month
Critical	9.0 - 10	Within 48 hours at the latest	2 weeks

10.2. The Supplier shall ensure hardening of the systems and software in line with the CIS benchmark hardening standards (and if these are not available, according to the supplier's hardening standards) in order to safeguard a secure configuration.

10.3. The Supplier shall conduct periodic automatic checks for any missing patches using a tool on the systems to verify whether security patches are being implemented according to the above schedule and shall report in relation to this.

a. Monthly reports will be prepared detailing the status of the latest patches and hardening operations. This report will be prepared by the Supplier and provided to SNBV on request.

b. The report will include information on the latest patches released, which systems have been patched and which systems are yet to be patched. In addition, information will be provided on the hardening operations that have been carried out, which systems have been hardened and which systems are yet to be hardened.

10.4. The Supplier will immediately notify SNBV in the event critical vulnerabilities are discovered and additional measures will be promptly taken to remedy these vulnerabilities.

10.5. The Supplier shall maintain a release calendar for all the software and hardware referred to above and shall anticipate 'end of life' notifications by discussing an appropriate upgrade project with SNBV at least 12 months before support is due to expire.

11. Account management

11.1. The Supplier is obliged to use the SNBV Identity Access Management environment (SCIM compliant) for account management, for the products and/or services supplied under the Agreement.

11.2. If the Supplier is unable, or is no longer able, to comply with the SNBV Identity Access Management procedure, the Parties shall jointly discuss an alternative account management procedure, after which the Supplier shall submit the proposal for an alternative procedure to SNBV for acceptance. After written acceptance of this alternative by SNBV, the Supplier shall ensure that it has and maintains formal procedures for the timely creation, modification and deletion of administration and other accounts, with 'timely' in this context understood to mean within 92 calendar days.

12. Destruction of data

12.1. In addition to the provisions in the Agreement pertaining to personal data, the Supplier shall not retain any other data obtained from SNBV under or in connection with the Agreement for longer than necessary and shall destroy such data upon the expiry of the Agreement or at SNBV's request, with due regard for the statutory retention periods.

12.2. On contract termination the revocation of physical and logical access rights to the organisation's information is executed.

12.3. The Supplier is obliged to assist with the data migration to another supplier or to the SNBV own systems.

13. Continuity

The Supplier shall implement all necessary IT technical measures to prevent or restrict the loss of availability or loss of integrity of network and information systems and in this way safeguard the continuity of its obligations to provide products and/or services under the Agreement to SNBV. Appropriate measures include implementing a robust backup system to prevent data loss, establishing and regularly testing a disaster recovery plan, and guaranteeing the availability of sufficient and qualified staff to safeguard service provision, even in case of illness or absence of key personnel.

14. Business assets/equipment

14.1. Any data that may still be present on any devices of the Supplier containing storage media, such as laptops or smartphones, must be deleted by the Supplier before the device is destroyed or reused. The data must be irreversibly deleted or, if the media cannot be irreversibly deleted, the media must be irreparably and demonstrably destroyed.

14.2. The Supplier shall ensure that the sensitive data are not disclosed to unauthorised parties.

14.3. The Supplier shall have a Bill of Materials. If requested by SNBV, it must be possible to indicate whether specific components are used.

15. Security incidents

15.1. If the Supplier has identified any security incident relating to information, business assets and systems (of SNBV and/or the Supplier) or the provision of services under the Agreement, the Supplier must report this to the SNBV ICT Service Desk exclusively and immediately, and in any event within 24 hours after the Supplier became aware of such security incident.

15.2. The Supplier must address notifications pursuant to this Cyber Security Annex to the SNBV ICT Service Desk:

IT Service Desk
Tel. +31 (0)20 6014445
e-mail: itservicedesk@schiphol.nl

The ICT Service Desk can be contacted by phone 24 hours a day, 7 days a week. If a notification is made pursuant to this Cyber Security Annex, the Supplier must also inform the contact person stated in the Agreement of the notification.

15.3. A notification to the ICT Service Desk must contain at least the following information:

- Start time and end time, start date and end date and the location of the event;
- Nature and extent of the event;
- Department or part of the system involved in the event;
- The time required to determine the loss and/or damage caused by the incident;
- The nature and extent of the data affected;
- Type and (estimated) number of data subjects, components and systems that were affected;
- The expected consequences, including the consequences for the data subjects, components and systems, and a proposal for preventing loss and/or damage and other adverse consequences;
- Measures that have been or will be taken to mitigate the consequences of the incident; and
- The name and contact details of the Data Protection Officer or other contact person from whom additional information on the incident can be obtained.

15.4. If requested by SNBV, the Supplier must permit and support an investigation of the information security incident.

16. ECAC Common Evaluation Practice approved resources

Security components approved by the "European Civil Aviation Conference" (ECAC) and based on the "Common Evaluation Process" are exempt from best practices/standards and any future changes if this compromises or endangers the Common Evaluation Process approval. The Supplier is obliged to notify SNBV in a timely manner regarding this matter so that the Parties can agree on additional measures.