EindhovenAirport

Security Annex

Edition 12-3-2025

Security Annex

Reliable information and digital solutions are crucial to fulfil the purpose of Eindhoven Airport; In addition, we must comply with the constantly evolving laws, regulations and standards.

With this Security Annex we formally give cyber security an active and visible place within our organization and we commit ourselves to a high level of cyber security towards all our stakeholders.

Colophon

Security Annex
Edition 12-3-2025
Version 8.0
Classification Public

Eindhoven Airport N.V.
Office Luchthavenweg 13
Terminal Luchthavenweg 25,
5657 EA Eindhoven

Security Annex

Inhoudsopgave

Chapter 1

About this document

This Security Annex contains the key security controls that we require from the contractors in the provision of products and/or services, and is included as an annex to the main agreement.

Limitation: *The contractor is solely responsible for what is within the sphere of its influence;*

A. The contractor is obliged to adopt and implement all cyber security measures relating to the execution of the Assignment that can reasonably expected of the contractor and that comply with the industry good practices applying at that time.
   The following shall also be understood to be referred to by 'contractor': its staff and any third parties engaged by it, including subcontractors, sub-assignees, suppliers, advisers and financiers. The contractor shall adopt the aforementioned measures for its own account and risk.
B. Following formal contract formation, the risks related to the system or service will be identified through a Business Impact Analysis. The resulting cyber security requirements will then be implemented by the contractor.
C. More specifically, the contractor's cybersecurity measures must include, at a minimum:

Chapter 2

Managing information security risks

1.1 The contractor is responsible for managing all cyber security risks that occur, or may occur, in connection with the execution of the Assignment by the contractor. In that connection, the contractor shall pro-actively identify all information security risks and adopt and evaluate measures to limit and/or mitigate cyber security risks.

1.2 The contractor shall at least once a year verify whether the service provided by it in connection with the Assignment complies with the provisions set out in this Security Annex and will upon request report to EANV on the extent to which its organisation complies with the provisions of this Annex.

1.3 As a contractor, you are required to handle our company information with care and confidentiality. It is strictly prohibited to process, input, or share sensitive or company confidential data within generative AI systems or external AI platforms without prior approval from EANV.

1.4 If the contractor identifies a risk with regard to (safeguarding) the confidentiality, integrity and availability of information, business assets, systems of and the service provision to EANV, the contractor is required to inform EANV thereof in writing as soon as possible but no later than within 7 days. Such a notification shall contain as a minimum:

   a. the risk to which EANV is exposed.
   b. the proposed control measures to mitigate, avoid or transfer the risk and the date/time by which these will be applied at the latest.

Requirements for contractor's staff and third parties engaged

2.1 The contractor shall ensure that all staff and third parties engaged by it that are involved in the execution of the Assignment have received the appropriate training in the field of information security in connection with their position and in view of the responsibilities when carrying out the work in connection with the Assignment. In order to be able to comply with this obligation, the contractor shall in any case arrange a security awareness programme, training programmes and activities on the basis of applicable good practices. In addition, the contractor shall inform the members of staff and third parties engaged that are involved in the service provision of the requirements set by EANV in this Security Annex.

2.2 The contractor shall ensure that, prior to the commencement of the Assignment, a background check has been carried out for the members of staff and/or third parties engaged that are involved in the execution of the Assignment. These persons/organisations will only be given access to the information, business assets, systems and service provision of EANV (that is/are relevant to the Assignment) 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 EANV's information, business assets, systems and services. In particular, a "Verklaring van Geen Bezwaar voor Burgerluchtvaart (VGB)" is required for staff and/or third parties engaged who will – for the purpose of the Assignment – get access to secure areas, 'high privileged accounts', critical information systems and/or sensitive information of EANV.

2.3 The contractor must have a formal disciplinary procedure in place for staff and/or third parties engaged who have committed a security breach or who do not meet EANV's information security requirements (as set out in this Security Annex), in accordance with prevailing good practice. In serious cases of misconduct, this procedure must provide for the immediate suspension and revocation of access rights and privileges relating to EANV's information and systems. The contractor is required to report such cases in writing to EANV without delay.

Access control

3.1 The staff and third parties engaged that are involved in providing the services shall only have access to those parts of EANV's information, business assets and systems as well as service provision locations that are required for the performance of their work within the scope of their position and in connection with the Assignment (the *least privilege* principle).

3.2 The contractor shall ensure that each account is personal – i.e. assigned to an individual user and not to a team or department – to ensure that all actions are traceable to individual users. Group accounts are not allowed.

3.3 The contractor must maintain a list of all the staff and third parties engaged that are involved in providing the services who have access to EANV's information, business assets and systems. During the provision of services, the contractor must check this list at least every 90 days to guarantee that the principle of *least privilege* remains in force and that any remaining/redundant accounts are deleted.

Penetration tests, audits, technical risk assessments

4.1 In consultation with the contractor and insofar as permitted with regard to costs and planning, EANV can carry out, or arrange for independent third parties to carry out, risk analyses (e.g. penetration tests), technical risk assessments, security scans (e.g. PCI compliance scans) and

audits on the service provision of the contractor – including and exclusively information systems that process EANV data. The contractor shall make available any information security documents, standards, process descriptions, documentation and information that are relevant to those activities. The contractor shall implement, within the agreed time line, corrective actions further to the findings that are identified during audits/technical risk assessments carried out by EANV.

Network, Communications and Endpoint security

5.1 The contractor must put control measures in place to protect the confidentiality and integrity of the data transmitted via public or wireless networks in accordance with the current state of the art, as well as to protect the connected systems and applications. Appropriate measures include, but are not limited to, Firewalls, Proxys, IDS/IPS, network segmentation and monitoring solutions.

5.2 The contractor must put control measures in place to protect all endpoints used for the ser-vice (e.g. servers, workstations and laptops) against malware, by deploying anti-malware management software for which the signatures are automatically updated at least daily, and by monitoring the network for suspicious activity.

5.3 The contractor is required to use cryptographic processing to protect the personal and other data it processes. It shall apply encryption when transmitting personal or other data across networks, when storing personal or other data on portable devices and on removable media, such as USB sticks, and in other situations where personal or other data are vulnerable to access by unauthorised persons (such as personal or other data that can be accessed through the internet. Examples of certified technologies are VPNs, SSH or HTTPS, or an equivalent technology for network security).

a. Secure technologies such 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. For websites, web applications and web services, the contractor shall use secure connections such as HTTPS so that the network traffic between the client and the web server is protected against access or modification by third parties.

c. The contractor shall ensure that its websites, web applications and web services use TLS 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.

Passwords

6.1 The contractor shall ensure that the passwords of all accounts (of both administrators and users) are stored with a secure one-way-hash mechanism such as SHA-2 or SHA-3 with a 'salt' addition.

6.2 The contractor shall ensure that passwords for user accounts with access to EANV data and systems are strong, which means at least 12 characters long and no repeating pattern. These passwords must be renewed within a maximum period of 180 days, where the last 10 passwords may not be reused.

6.3 Passwords for administration accounts that are used by the contractor must be very strong, which means at least 15 characters long and no repeating pattern. These passwords must be

renewed within a maximum period of 180 days, where the last 10 passwords may not be re-used.

6.4 Passwords for service accounts – which are not used by a human user by rather by another system/application, e.g. for data exchange or automated tasks – must be very strong, which means at least 24 characters long and no repeating pattern. These passwords must be renewed within a maximum period of 5 years, where the last 10 passwords may not be reused.

Multi-factor authentication

7.1 Multi-factor authentication must be used for 'high privileged accounts' of the contractor, for access to systems processing personal or other sensitive data, and for remote access via the internet.

7.2 Multi-factor authentication must be used for user accounts and administration accounts with a password validity of more than 180 days.

Patching, End-Of-Life software & hardening

8.1 The software used or supplied by the contractor (OS, database, middleware and application software) shall feature all the known security patches issued by the contractor, 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

8.2 Operating systems or applications that are end-of-life should not be used. This is because security patches are no longer released by the vendors.

8.3 The contractor shall ensure hardening of the systems and software in line with the CIS standards (or the security standards of the supplier) in order to safeguard a secure configuration.

Account management

9.1 The contractor shall ensure that it has and maintains formal procedures for the timely creation, modification and deletion of (administration) accounts. An account that has not been used for 90 days must be deactivated or deleted.

Destruction of data

10.1 The contractor shall ensure that data is destroyed in a timely manner and in accordance with the (statutory) retention period.

Equipment

11.1 Any personal or other data of EANV that may still be present on any devices of the contractor containing storage media, such as laptops or smartphones, must be deleted by the contractor before the device is destroyed or reused. The personal or other data must be irreversibly deleted or, if the data cannot be irreversibly deleted, the media must be irreparably destroyed.

11.2 The contractor shall ensure that the personal data or other sensitive data are not disclosed to unauthorised parties.

Security incidents

12.1 Whenever the contractor identifies any actual or presumed security incidents relating to information, business assets, systems or the provision of services, the contractor must report them to EANV exclusively and immediately, but in any event within 24 hours after the contractor became aware of them.

12.2 A notification to the IT Service Desk must at least contain the following information:

- the start time and end time, start date and end date and the location of the event;
- the nature and extent of the event;
- the department or part of the system involved in the event;
- the time required to determine the loss caused by the incident;
- the nature and extent of the (personal) data affected;
- the type and (estimated) number of Data Subjects that were affected;
- the expected consequences, including the consequences for the Data Subjects and a proposal for preventing loss and other negative consequences;
- the 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.

12.3 If requested by EANV, the contractor must permit and support an investigation of the information security incident.

Notifications pursuant to the Security Annex

13.1 Notifications pursuant to this Security Annex must be addressed to EANV's IT Service Desk:

IT Service Desk
Tel: +31 (0) 40 – 2919847
Email: IT@eindhovenairport.nl

The IT Service Desk can be contacted by telephone 24 hours a day, 7 days a week.

13.2 If a notification is made pursuant to this Security Annex, the contractor must also inform the contact person appointed in the Agreement about this.