Security Annex

1. **Managing information security risks**

   The Other Party is responsible for managing all information security risks that may arise in the context of the performance of the Main Agreement and the processing of data by the Other Party, its employees and any third parties it may engage (including subcontractors, suppliers and advisers). In this context, the Other Party must proactively identify all information security risks, adopt and evaluate measures to mitigate these risks (the "**Security Measures**"). The Other Party will, upon request from EANV, demonstrate that adequate Security Measures have been adopted.

2. **Training employees and third parties engaged by the Other Party**

   The Other Party will ensure that all employees involved in implementing the Main Agreement and the processing of data and any third parties it may engage have received the relevant information security training/awareness based on their roles and responsibilities in performing work under the Main Agreement and the processing of data. To comply with this obligation, the Other Party will run a security awareness programme, together with education and training activities on a regular basis based on good practice. Also, the Other Party will inform all employees and any third parties it may engage about the requirements that are set out in this annex.

   The Other Party shall have formal disciplinary procedures in place for employees and third parties it may engage, which committed a security breach or do not comply with information security requirements of EANV (as set out in this security annex), in accordance with applicable good practices. In case of serious misconduct should these procedures result in immediate suspension and withdrawal of the access rights and privileges to the information and systems of EANV. The Other Party shall report such cases immediately in writing to EANV.

3. **Network and communication security**

   The Other Party shall take measures to ensure the confidentiality and integrity of data that is being transmitted via public networks or wireless networks in accordance with the latest security technology standards and to protect connected systems and applications. Valid measures are for example firewalls, proxies, intrusion detection/protection systems, network segmentation, anti-virus/anti-malware/anti-ransomware systems and monitoring solutions.

The Other Party applies cryptographic processing to protect the data it processes. Encryption must be applied when data is being transferred across public and/or from the internet-accessible networks and stored on fixed, portable devices or removable media such as USB sticks, and in other situations where data is vulnerable to unauthorised access (such as data that can be accessed through the World Wide Web). Approved technology types include VPNs, SSH or HTTPS, or an equivalent technology for network security.

a. Secure technology such as Advanced Encryption Standard (EAS) technology with 256-bit keys or longer 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 misused.

b. When using a website, the Other Party must use HTTPS to make network traffic between the client and the web server unreadable by third parties if the data is sensitive or personal. The processor will give EANV the opportunity to perform audits at any time desired by EANV, including, but not limited to Qualys SSL server test with at least an A score.

c. The Other Party will ensure that its website is protected by using an SSL/TLS certificate issued by a recognised public Certificate Authority (CA) such as Digicert, VeriSign, etc. 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.

4. Password security

The Other Party will ensure that passwords of all accounts, for both administrators and users, are stored with a secure one-way-hash mechanism (such as SHA-2 or SHA-3) with a "salt" addition.

5. Password rules

The Other Party will ensure that the passwords for user accounts are strong (60 bit entropy), and contain at least the following complexity:

(i) at least 8 characters and made up of at least three of the following categories:

a. upper-case letters (A-Z),

b. lower-case letters (a-z),

c. figures (0-9),

d. special characters such as ! # $ ^ * - _ = ; ⁄ " ( ) { } [ ] | ` @ % & ? / \ +; or

(ii) at least 14 characters and made up of at least two of the following categories:

a. upper-case letters (A-Z),

b. lower-case letters (a-z),

c. figures (0-9),

d. special characters such as ! # $ ^ * - _ = ; ‘ " ( ) { } [ ] | ` @ % & ? / \ +

These passwords must be changed at least once every 92 days. This requirement must be enforced through the IT service provided by the Other Party.

Passwords for administrator accounts used by the Other Party must be very strong, and must contain at least the following complexity: at least 15 characters and made up of at least three of the following categories:

a. upper-case letters (A-Z),
b. lower-case letters (a-z),
c. figures (0-9),
d. special characters such as ! # $ ^ * - _ = ; ‘ " ( ) { } [ ] | ` @ % & ? / \ +

These passwords must be changed at least once every 180 days.

6. Multi-factor authentication

Multi-factor authentication technology must be used if the Other Party’s administrators require remote access via public networks, such as the Internet, to the systems on which personal or other data is processed or stored.

7. Patching and hardening

All known security patches released by the Other Party, developer or programmer have been applied to the software used by the Other Party (OS, database, and application software).

The Other Party ensures hardening of systems and software in accordance with CIS standards (or the security guidelines of the manufacturer) to ensure a safe configuration.

8. Account management

The Other Party has formal procedures in place for creating, changing and deleting accounts. In particular, it is important that accounts are deleted from the IT service in a timely manner. Any account that has not been used for 90 days must be disabled or deleted.
When an account is deleted, all related data must be irreparably erased unless the operation of the application will be disrupted. In that case the Other Party must contact EANV’s IT Service Desk (it@eindhovenairport.nl). These data must also be deleted from the backup. *Remark: it is allowed that data may exist in a back-up for maximal 35 days.*

9. **Data minimization**

   The processor applies data minimization, which means that the processing of data is reduced to the utmost necessity.

10. **Retention**

    The Other Party will ensure that data is destroyed in a timely manner and in accordance with the agreed retention periods. In case of Personal Data or transactional data could also be done by anonymizing data. The method of anonymization must always be in consultation with EANV.

11. **Procedures for handling information security incidents**

    The Other Party has written procedures for promptly and effectively processing information security incidents and identified vulnerabilities in the security. The Other Party had the obligation to immediately report to EANV any information security incidents detected and identified vulnerabilities within 24 hours after the Other Party is known with this information.

12. **Audit IT system**

    When the IT system containing the Personal Data is delivered, EANV can carry out an audit or arrange to have an audit carried out to check whether the security of these IT resources had been set up in a technically correct manner and in accordance with the above requirements. The Other Party must facilitate this audit. As an alternative, EANV may use a statement by an independent external expert who gives an opinion on the measures taken by the Other Party (Third Party Assurance).

13. **Erasing data and equipment**

    The Other Party must erase any remaining personal or other data from any of its devices containing storage media, such as laptops or smartphones, before the devices are destroyed or reused. The personal or other data must be securely erased or, if the media cannot be securely wiped (such as an SSD), it must be securely destroyed.

14. **Access management**

    All employees and engaged third parties shall only have access to those parts of the information, company assets, systems, and facilities of EANV that are strictly required for the fulfilment of this agreement (so-called least-privilege principal).