APPENDIX (B)

Information Security Annex (ISA)

INTRODUCTION

The purpose of this ISA is to identify the minimum-security requirements to which the supplier shall commit.

PRIORITY OF DOCUMENTS

This ISA prevails over the Supplier's security policies whether or not referenced or attached to the Contract.

This ISA is a standard document that applies to any and all Agreements that make reference to this ISA. However due to the standardized nature of this document the following shall apply:

i. The Agreement shall prevail over the ISA. The ISA shall be supplementary and subsidiary to the Agreement, even in cases where a different order of precedence has been set out in the Agreement.
ii. All terms written in capital letters shall be interpreted (I) in the first place, according to the definitions at the end of this ISA and (ii) by default, as defined in the Agreement containing the reference to this ISA.
iii. Deliverables as listed in this ISA shall mean any product and/ or service ordered based on the main Agreement including all main- and ancillary obligations.

1 GENERAL APPLICABILITY

The Supplier shall comply with ISA requirements for Deliverables according to the following table:

Deliverable	Section A Technical Security	Section B Organizational Security	Section C Operational Security
Software	Applicable	Applicable	Applicable
Hardware	Not Applicable	Not Applicable	Not Applicable
Service	Applicable	Applicable	Applicable

2 A. TECHNICAL SECURITY

3 Security by Design

In order to minimize the attack surface of Deliverables, the Supplier shall:

- respect state-of-the-art security configuration practices (such as https://www.cisecurity.org/) or third-party security best practices applicable to each Deliverable; design Deliverables to use only necessary components, features, and services (e.g., by removing unnecessary files, process permissions, libraries, and network ports); and Ensure that Deliverables do not contain any Back Doors.

Each Deliverable shall:

- be free of Vulnerabilities listed in the “CWE/SANS Top 25” (http://cwe.mitre.org) at the time the Agreement is agreed or renewed;
- be robust against unexpected inputs (such as SQL Injection); always act in a predictable way even in overload situations; and
- Use standard cryptographic algorithms recommended by institutions (such as BSI, ANSSI and NIST) at the time the Contract is agreed or renewed.
- The Supplier shall deliver evidence about the security of each Deliverable such as security audit reports, vulnerability scans and code robustness analyses.
- Software and Hardware Deliverables shall allow authentication data (such as passwords) and cryptographic keys to be modifiable according to state-of-art robustness by the TCSI & CBSI and MNO's.
- The Supplier shall implement the mutually agreed security Statement of Compliance applicable for this project.
- The Compliance of the ISA Requirements Shall be Verified by a Certified Organization recognised by International Regulatory Bodies especially (PCI DSS)

4 Vulnerability Management

The Supplier shall put a Vulnerability and Advisory Management System in place being capable - among others - to monitor security advisory sources to get informed of new Vulnerabilities (including third-party components) that could impact the Deliverables.

Where appropriate, each Vulnerability shall have a unique CVE identifier associated with the CVSS score (V2 or above). Any alternative must be agreed with the TCSI and the project partners.

The Supplier shall promptly provide information to the TCSI about each Vulnerability and its consequences (e.g., CVE, CVSS score, affected component or services)

Unless otherwise agreed in the Agreement, the Supplier shall fix Vulnerabilities according to the following table:

CVSS Score	Classification	Temporary Fix time	Official Fix time
7.0 – 10.00	Critical	5 working days	1 month
4.0 – 6.9	Major	10 working days	3 months
0 - 4	Minor	N/A	6 months

Temporary Fix time: the maximum time needed for a Temporary Fix. The time counter starts when the Vulnerability is discovered. If a Temporary Fix is not possible, the Supplier shall suggest a workaround with best-effort approach.

Official Fix time: the maximum time needed for the Official Fix. The time counter starts when the Vulnerability is discovered, except for third party Vulnerabilities where the time counter starts when a patch is available.

There may be occasions requiring a faster response than the above table (e.g., press publication of Vulnerability in a Deliverable used by the TCSI and MNO's with a

significant brand impact on the TCSI and MNO's). For Vulnerabilities in the technical environment necessary to operate the Deliverable (e.g., OS for a Software Deliverable), the Supplier shall employ commercially reasonable efforts to support the TCSI and MNO's to fix such Vulnerabilities.

5 Security Patch Management

For Software and Hardware Deliverables, the Supplier shall provide security patches not older than 6 months at the following times:

- at the date of delivery of the Deliverable
- at the start of Acceptance tests if there is an Acceptance procedure
- before “go live” if there are no Acceptance tests
- during the life cycle of the Deliverable

The Supplier shall deliver at least 2 security releases per 12-month period to bundle major and minor patches if necessary and provide information (e.g., CVE, CVSS score) about the Vulnerabilities that have been fixed.

For Service Deliverables, the Supplier shall:

- implement a patch management process (including patch testing)
- apply security patches promptly and guarantee that security of the Service is not altered

6 B. ORGANIZATIONAL SECURITY

7 Point of Contact

The Supplier shall nominate both, a contact person for security related matters and an upper-management contact or key-account manager to handle escalation matters. The contacts shall be provided for each project and changes shall be communicated promptly.

8 Security Incidents

The Supplier shall promptly notify the TCSI, CBSI and MNO's in case an incident related to the Supplier may have an impact on the TCSI & CBSI and MNO's (for example, loss, alteration, disclosure or non-authorized access to source code, data, personal data, or information, etc.).

The Supplier shall use all efforts to remediate and/or solve the incident and inform the TCSI & CBSI of progress and end-of-incident.

9 Access to TCSI & CBSI’s Systems

If the TCSI & CBSI grants the Supplier access to their systems, the Supplier shall:

- be responsible for any actions performed on the Assets of the TCSI & CBSI under user and Service Accounts attributed to the Supplier;
- comply with any process and means of remote access provided by the TCSI & CBSI;

- ensure that there is no breach of confidentiality, availability or integrity on any Assets or services whilst remotely connected to TCSI & CBSI technical and operational systems
- Ensure unique accounts for every user. Exceptions must be agreed in writing by the TCSI & CBSI;
- promptly notify the TCSI & CBSI when a user account is no longer required;
- provide a periodic user account review report at minimum once a year; and
- Ensure that Service Accounts are not used by individuals to log in to TCSI & CBSI systems.

10 Documentation

The Supplier shall deliver to the TCSI & CBSI all necessary information to assess the security of Deliverables and to securely configure the Deliverables. The Supplier shall keep the documentation delivered to the TCSI & CBSI up to date.

11 Asset Management

The Supplier shall identify, document, and protect all Assets (information, software, hardware, computers, USB stick, badge, tablet, smartphone…) of the TCSI & CBSI that have been entrusted to the Supplier.

12 Human Resources Security

The Supplier shall ensure that its employees and any third parties appointed by the Supplier for the performance of the Agreement:
- possess the appropriate security skills; and
- know and implement the applicable security rules for the performance of tasks.

Upon request of the Supplier, the TCSI & CBSI shall provide the applicable security rules before the start of any tasks.

Anybody acting on behalf of the Supplier, who needs remote or local access to the TCSI & CBSI's information system, is required to provide identification information. The Supplier shall ensure that any access on his behalf is not abused and assumes full responsibility for it.

Where the Supplier uses subcontractors to fulfil the Agreement with the TCSI & CBSI, the Supplier shall specifically identify them as subcontractors and ensure that the same due care will always be applied.

Upon request of the TCSI & CBSI, the Supplier commits to use only security checked personnel, i.e. screened by national authorities, for handling of sensitive Deliverables prior to deployment in the TCSI & CBSI's Network, as well as for maintenance of sensitive Deliverables during the whole operational phase.

13 Security Audits

The TCSI & CBSI or any third party assigned by the TCSI & CBSI shall have the right to undertake audits in order to check Supplier's compliance with the TCSI & CBSI's security requirements defined in the Agreement.

14 Organization of Information Security

The Supplier shall apply an enterprise information security policy as a standard approach according to ISO/IEC 27001 or any other standard.

If the Supplier is certified, the Supplier shall provide its security certification and keep the TCSI & CBSI informed of renewals or revocations of its certificates.

Upon request of the TCSI & CBSI, the Supplier shall provide information about his security organization.

15 Failure to Comply with this ISA

15.1 Material Breach of Contractual Obligations

Failures by the Supplier to comply with the commitments described in this ISA will be treated as material breach of the Agreement.

15.2 Liquidated Damages/ Penalties

Further to the remedies as a consequence of a material breach as set out in section 15.1 above, the TCSI & CBSI may apply liquidated damages or penalties to the Supplier.

Unless otherwise agreed in the Agreement, the following liquidated damages shall (additionally) apply in the case of Vulnerabilities:

If the Supplier fails to deliver a security Official Fix for Vulnerabilities with a CVSS score greater than 7 as per the table defined in section A.2 “Vulnerability Management”, the liquidated damages are calculated as follows:

A = V x N / 300
A: amount of liquidated damages.
V: If the Vulnerability is located on the Service, V is the global cost of Service per year for TCSI & CBSI. If not, V is the value of the Deliverables.
N: number of calendar days exceeding the Official Fix deadline.

16 C. OPERATIONS SECURITY

16.1 Information and Access Management

The Supplier shall process, use, and transmit TCSI & CBSI information involved in the Service only for Service provision and only for the duration of the Agreement.

The Supplier shall ensure that:

- access to TCSI & CBSI information is based on a strict “need-to-know” basis;
- Access to TCSI & CBSI information logged and retained for the duration agreed in NPA and/ or Order including associated documents (e.g., Non-Disclosure Agreement or Data Protection Agreement) or 6 months by default. Extracts of retained logs shall be provided to the TCSI & CBSI on request; and
- Unauthorized access (e.g. by other customers or third parties) to TCSI & CBSI information does not occur under any circumstances.

In the event of a security incident, TCSI & CBSI may suspend access or request suspension of access until the incident is resolved.

In addition, the Supplier shall implement the following measures on information classed as confidential by the TCSI & CBSI:
- data shall be encrypted when stored and transmitted; and
- A strong authentication system shall be implemented.

16.2 Business Continuity Management

The Supplier shall implement in compliance with the maintenance conditions agreed in the Agreement, all necessary means (architecture, event detection and response, backup plan, continuity plan…) to protect the Services from unwanted or voluntary incidents that could threaten the continuity of the Services.

16.3 Separation of Development, Testing and Production Environments

The Supplier shall separate development, testing and production environments and shall not use production data for testing activities.

16.4 Reporting

The TCSI & CBSI may request from the Supplier a security report related to the Services no more than twice a year. This security report shall include but is not limited to the following information:
- the number of security incidents detected over the last 12 months, separately for internal and external causes if relevant;
- details of security incidents over the period (detection time, nature and impact, solution, service recovery time, closing time, time for resolution); follow up of action plans; and
- Future scheduled operations and Service evolutions that may impact the security level.

16.5 Use of Third Party Services

The Supplier shall inform the TCSI & CBSI if Third Party services (e.g. data center services) are involved or planned to be involved in the provision of the Service. The Supplier shall ensure that Third Party services are always compliant with the security requirements applicable to the Service.

DEFINITIONS AND ABBREVIATIONS

Assets	encompass - as defined in ISO/IEC 27005 - primary and supporting assets.
Back Door	means a feature or defect of Deliverables that allows surreptitious unauthorized access to data.
CVE	means Common Vulnerabilities and Exposures as defined in: http://cve.mitre.org/index.html
CVSS	means Common Vulnerability Scoring System as defined in http://www.first.org/cvss/
Deliverables	mean any equipment, product and/or service ordered on the main Agreement including all main- and ancillary obligations.
Information Security	means - in compliance with ISO/IEC 27001 and ISO/IEC 27005 - security in the scope of information processing and activities (primary assets) relying on technical (including, but not limited to IT, premises, facilities, networks) and non-technical resources (including, but not limited to supporting assets such as staff, partners, organizations, procedures, terms, and conditions).
Official Fix	means that a complete vendor solution is available to fix a Vulnerability, either by means of an official patch or an upgrade.
OS	means Operating System.
Service Account	means a special user account that is created explicitly for a Service.
Temporary Fix	means that there is an official but temporary fix available to fix a Vulnerability, including – but not limited to - temporary hotfixes, tools, or workarounds.
Vulnerability	means a weakness that reduces availability, integrity, or confidentiality.