Information Security Annex

GENERAL PRINCIPLES

This Information Security Annex (ISA) establishes the information security measures of Deutsche Telekom AG (DTAG). If applicable to the Deliverables listed in the Agreement, the Supplier must consider these measures as a minimum of security standard and they must apply for the duration of the Agreement, regardless whether the Deliverables are procured with reference to the Agreement from the Supplier or via third party distributors.

These measures cover different aspects of information security and some are applicable depending on the nature of the Deliverables set out in the Agreement.

In addition, these measures may be reinforced with additional security measures which will be provided by the Purchaser and agreed between the parties in documents attached to the Agreement, a NPA and/or an Order.

PRIORITY OF DOCUMENTS

This ISA is a standard document that applies to any and all Agreements entered into with the Supplier that make reference to this ISA.

The following shall apply:

1. The Agreement shall prevail over the ISA, unless a different order of precedence has been set out in the Agreement; and

2. Notwithstanding the above, all terms written in capital letters shall be interpreted according to the definitions at the end of this ISA and by default as defined in the Agreement containing the reference to this ISA.

The Parties agree that this ISA shall further prevail over Supplier documents defining security measures attached to or referenced in the Agreement, a NPA and/or an Order.

GENERAL APPLICABILITY OF ISA

The Supplier shall comply with ISA requirements for all Deliverables as defined in the following:

– **Software** refers to off-the-shelf vendor software and/or custom software resulting from a Statement of Work mutually agreed by the Parties (e.g. Software Result);

– **Hardware** including any embedded software/firmware (e.g. IT equipment, network equipment, etc.);

– **Customer Equipment** including any embedded software/firmware (e.g. end-user equipment, mobile phones, mobile broad band, tablets, end-user connected devices, mobile CPE, mobile devices for Internet of Things, connected watches, smart TV, gateways, set-top boxes, repeaters, etc.);

– **XaaS/Cloud Services** (e.g. Software as a Service); and

– **Professional Services** for performing installation, training, integration, maintenance and/or consulting.

GENERAL APPLICABILITY OF SPECIFIC SECTIONS REGARDING THE DELIVERABLES

The following sections are applicable to any kind of Deliverable:

– **Section A: "**Contractual and standards compliance"

– **Section B: "**Security organization"

– **Section C: "**Incident management**"**

The following sections apply according to the nature of Deliverables as defined in table A:

- **Section D:** "Cryptography and authentication"
- **Section E:** "Security by design"
- **Section F:** "Software Vulnerabilities fixing"
- **Section G:** "Purchaser Data in XaaS/Cloud Services"
- **Section H:** "Access control of XaaS/Cloud Services"
- **Section I:** "Operations of XaaS/Cloud Services"
- **Section J:** "Access to and use of Purchaser systems and resources"
- **Section K:** "Professionals and security"
- **Section L:** "Distribution of software updates"

Deliverable	Applicable sections
Software	A, B, C, D, E, F
Hardware	A, B, C, D, E, F
XaaS/Cloud Services	A, B, C, D, E, F, G, H, I
Customer Equipment	A, B, C, D, E, F, L
Professional Services	A, B, C, J, K

Table A: Applicability of ISA sections

A   CONTRACTUAL AND STANDARDS COMPLIANCE

A.1 Security assessment of Deliverables

Upon request of the Purchaser, the Supplier shall provide the Purchaser within 10 working days all necessary information to assess the security of Deliverables such as security test/audit reports, vulnerability scans and code robustness analyses.

A.2 Security policies

The Supplier shall apply an enterprise information security policy according to ISO/IEC 27001 standard or similar industry-recognized practice.

If the Supplier is certified, it shall provide the Purchaser with its security certification and keep the Purchaser informed of renewals or revocations of its certificates.

If the Supplier was selected by the Purchaser based on a certification (e.g. ISO/IEC 27001), the Supplier shall maintain such certification during the entire term of his contractual duties.

A.3 Audit

The Purchaser and DTAG shall have the right to undertake audits to check Supplier's compliance with the Purchaser's and DTAG's security requirements as defined in the Agreement.

A.4 Third Parties

In case the Supplier uses Third Parties in providing the Deliverables to the Purchaser, the Supplier shall ensure that such Third Parties meet the security measures agreed in the Agreement.

A.5 NESAS Compliance

NOTE: This paragraph A.5 is only applicable to mobile network equipment (meaning equipment for mobile core network, RAN and mobile access).

Suppliers that offer mobile network equipment must undergo the NESAS (Network Equipment Security Assurance Scheme) vendor development and lifecycle processes assessment, as defined in the respective NESAS specifications, issued by the GSM Association (GSMA PRD FS.13/15/16), in the current version.

The Supplier must also provide DT with both the Audit Report and Evaluation Report, created as a result of the assessment, performed by a recognised auditor. The assessment must be completed prior to offering any mobile network equipment. Should the Supplier or Supplier's Deliverables be re-assessed, all the updated reports shall be provided.

A.6 Failure to comply with this ISA

In case Supplier becomes aware of a non-compliance with security measures in its Deliverables, the Supplier shall promptly provide the Purchaser with an analysis of the situation and a remediation plan. If the remediation plan is accepted by the Purchaser, it will be implemented by the Supplier at no cost to the Purchaser and the Supplier shall provide proof of remediation plan's efficiency.

If non-compliance persists or a remediation plan is not accepted or fails, this will automatically be deemed as a material breach of the Agreement.

B   SECURITY ORGANIZATION

B.1 Structure

Upon request of the Purchaser, the Supplier shall provide information about its security organization.

B.2 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 Order and changes shall be communicated promptly.

B.3 Security reviews

Once a year, upon request of one or both Parties, the Supplier and the Purchaser shall organize a meeting to review security aspects (e.g. evolutions and scheduled operations that may impact security).

Each Party can ask for an exceptional security meeting that shall be accepted by the other Party if the situation imposes a common analysis or immediate decision (for example a major incident or a significant evolution of threats).

B.4 Security measure for Purchaser data

Purchaser data is any kind of Purchaser assets e.g. business information (like contracts or business plans) or technical information (like network diagrams).

The Supplier shall implement the following measures on shared Purchaser data which is classified as confidential by the Purchaser, i.e. data encrypted by the Purchaser and/or marked as Confidential:

− such data shall be encrypted when stored and transmitted; and

− a strong authentication system (e.g. two-factor authentication system) shall be implemented.

The Parties shall agree in advance on a method of exchange in case of a need to exchange encrypted information.

C   INCIDENT MANAGEMENT

C.1 Detection

The Supplier shall have measures in place to detect security incidents impacting the Purchaser and occurring in the Supplier's environment. Security incidents include but are not limited to loss, alteration, disclosure or unauthorized access to Purchaser data or information and unauthorized disclosure of proprietary source code or other intellectual property rights.

C.2 Notification

The Supplier shall promptly notify the Purchaser in case of any such security incident.

Where a breach and/or misappropriation of Purchaser's data or information are determined, the Supplier shall notify the Purchaser according to applicable laws but within 24 hours latest.

Such security incident notification shall be sent to cert@telekom.de in addition to Supplier's Purchaser contact.

Details of security incidents shall be retained by the Supplier at least until the next security review between the Parties.

C.3 Resolution

The Supplier shall use best efforts to immediately resolve security incidents and inform the Purchaser of progress and end-of-incident.

C.4 Suspension of Supplier access to Purchaser systems

NOTE: This paragraph C.4 is not applicable to Software, Hardware, Customer Equipment Deliverables and XaaS/Cloud Services.

In the event of a security incident concerning Professional Services, the Purchaser may suspend Supplier access to Purchaser systems until the incident is resolved.

C.5 Suspension of Purchaser access to Xaas/Cloud Services

NOTE: This paragraph C.5 is not applicable to Software, Hardware, Customer Equipment Deliverables and Professional Services.

In the event of a security incident concerning XaaS/Cloud Services (e.g. system intrusion, malware incident), the Purchaser may suspend his access to the said Service until the incident is resolved.

In the event where the Purchaser is not able to suspend access, the Purchaser shall explicitly request the Supplier to suspend all Purchaser access until the incident is resolved. Supplier shall promptly comply with such request.

C.6 Security report for XaaS/Cloud Services and Professional Services

NOTE: This paragraph C.6 is not applicable to Software, Hardware and Customer Equipment Deliverables.

The Purchaser may request from the Supplier a security report related to the XaaS/Cloud Services and/or Professional 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; and

- details of security incidents over the period (detection time, nature and impact, resolution, service recovery time, closing time, time for resolution).

D CRYPTOGRAPHY AND AUTHENTICATION

D.1 Modification of authentication data and cryptographic keys by Purchaser

All authentication data and cryptographic keys (e.g. certificates, key pairs, symmetric keys, passwords) in Software, Hardware and Customer Equipment Deliverables shall be modifiable by the Purchaser and protected according to state-of-art. For authentication data and cryptographic keys that are not modifiable by the Purchaser, Supplier shall provide a list of such data and their purpose to the Purchaser. For XaaS/Cloud Services, this requirement applies only to authentication data used by the Purchaser for protecting its data including administrative accounts.

D.2 Strength of cryptographic algorithms and keys

The Supplier shall implement only standardised cryptographic algorithms and key lengths recommended by governmental institutions (such as BSI, ANSSI and NIST) at the time the Agreement is agreed or renewed and shall regularly update such standardised cryptographic algorithms and key lengths accordingly for new Deliverables.

E SECURITY BY DESIGN

E.1 Hardening

The Supplier shall employ system hardening best practices. This includes, but not limited to restricting protocol access, removing or disabling unnecessary software, network ports and services, removing unnecessary files, user accounts, restricting file permissions, patch management and logging.

The Supplier shall provide Deliverables (including Third Party components and services) that are securely configured by default according to state-of-the-art security configuration practices (such as https://www.cisecurity.org/).In addition, the Supplier shall ensure that Deliverables do not contain any Back Doors.

E.2 Testing for software security errors

The Supplier shall test the Deliverables to ensure that they are free of dangerous software errors listed in "CWE/SANS Top 25" (http://cwe.mitre.org) and/or "OWASP TOP 10" (http://www.owasp.org) at the delivery date (e.g. robustness against unexpected inputs such as SQL Injection, predictable behaviour in overload situations, etc.).

E.3 Documentation transparency

The Supplier shall provide the Purchaser with:

- the necessary documentation for secure configuration of the Deliverables and keep such documentation up-to-date;

- the Software Bill of Materials in machine readable format (including vendor name when applicable, software and/or open source name and version) and keep such inventory up-to-date.

E.4 Additional measures

Upon request of the Purchaser, the Parties may mutually agree on additional security measures that the Deliverables must satisfy.

These additional measures may be gathered in a document called "Security Statement of Compliance" and be included in the Agreement and/or in the NPA.

F   SOFTWARE VULNERABILITIES FIXING

F.1 Detection

The Supplier shall have measures in place to continuously monitor external security advisory sources (such as cooperative security tests, external security research, open source and third party disclosure, …) and track Vulnerabilities that could impact the Deliverables (including Third Party components).

F.2 CVE Standard

Where appropriate, each Vulnerability detected by the Supplier shall have a unique CVE identifier associated with a CVSS score (v3 or higher) consisting of the CVSS base, the temporal score and the vector id.

F.3 Notifications

The Supplier shall promptly provide information to the Purchaser about each Vulnerability (with CVSS score greater or equal than 7.0) including Zero-Day impacting the Deliverables and its consequences (e.g. CVE if exists, CVSS score, affected components or services).

The Supplier shall communicate security advisories in any parsable format (such as CVRF, CSAF, XML, JSON) via email :

All Deliverables	cert@telekom.de
Customer Equipment Deliverables	Same as above and equipmentsecurity@telekom.de

F.4 Service level agreement to fix Vulnerabilities

For each Vulnerability impacting the Deliverables, the Supplier shall:

- make all efforts to provide a Temporary Fix to the Purchaser according to the following table; and

- make the Official Fix available to the Purchaser according to the following table.

CVSS base score v3	The maximum time to provide a Temporary Fix	The maximum time to provide the Official Fix
From High to Critical 7.0-10.0	5 (five) calendar days	30 (thirty) calendar days
From Low to Medium 0-6.9	not applicable	6 (six) months

The time counter starts when the Vulnerability is detected, except for a Vulnerability located on Third Party components where the time counter starts when a fix is available.

F.5 Security maintenance of third party components

The Supplier shall ensure that all Third Party components used within the Deliverables are security maintained during the Lifecycle of the Deliverables.

F.6 Security Defects

The Supplier shall accept for each Vulnerability impacting the Deliverables and detected by the Purchaser during the contracted period of maintenance and/or warranty period that the Purchaser can open a maintenance ticket

to fix it. In addition to section F.4, the Supplier shall respect the maintenance conditions to correct the Defect related to the Vulnerability.

F.7 Exceptions

The Supplier shall employ commercially reasonable efforts to support the Purchaser to fix Vulnerabilities:

- in occasions requiring a faster response than the above table (e.g. press publication of Vulnerability in a Deliverable used by the Purchaser); and

- in the technical environment necessary to operate the Deliverables (e.g. operating system for a Software Deliverable).

F.8 Liquidated Damages/Penalties for Vulnerability fixes

In addition to the remedies as a consequence of a material breach as set out in section A.6 "Failure to comply with this ISA", the Purchaser may apply liquidated damages or penalties to the Supplier as per the sections "Liquidated Damages" or "Penalties" of the Agreement.

In case of Vulnerabilities the following liquidated damages scheme shall apply:

If the Supplier fails to provide a security Official Fix for Vulnerabilities with a CVSS score greater than or equal to 7 as per the table defined in section F.4 "Service level agreement to fix Vulnerabilities", the liquidated damages are calculated as follows:

$$A = V \times N / 300$$

A: amount of liquidated damages.

V: V is the value of the Deliverables.

N: number of calendar days exceeding the Official Fix deadline.

F.9 Security-related maintenance

The Supplier shall define for each Deliverable a minimum Support Period which cannot be smaller than the warranty period.

During the Lifecycle of the Deliverables, the Supplier shall provide the Purchaser with:
- Current Deliverables release and future releases with all security fixes;
- security fixes as and when they are released, respecting the Vulnerability fix times defined in section F4;
- information (e.g. CVE, CVSS score) about the Vulnerabilities that have been fixed.

G   PURCHASER DATA IN XAAS/CLOUD SERVICES

G.1 Limitation of use of Purchaser data

The Supplier shall use Purchaser data transmitted, processed, generated and/or stored in the XaaS/Cloud Service only to provide the said Service.

G.2 Segregation of Purchaser data

The Supplier shall enforce segregation of Purchaser data from data of other customers of the Supplier.

G.3 Purchaser confidential data

The Supplier shall encrypt in transit and in storage all data that is classified by the Purchaser as confidential and stored in Supplier's XaaS/Cloud Service.

G.4 Supplier encryption mechanisms

In case the Purchaser uses an encryption mechanism provided by the Supplier to protect Purchaser data, the Supplier shall ensure that:

− such data shall be kept encrypted when stored and transmitted; and

− a strong authentication (e.g. two-factor authentication) is used for access to such data.

G.5 Logging of Purchaser data access and use

The Supplier shall:

− log access to and usage of Purchaser data in the XaaS/Cloud Service, including by his employees and any appointed third parties; and

− retain such logs for the duration agreed in the NPA and/or Order including associated documents (e.g. Non-Disclosure Agreement or Data Processing Agreement) or 6 months by default.

Extracts of retained logs shall be provided to the Purchaser on request.

G.6 Purchaser Data reversibility

Upon termination of the NPA and/or Order, the Supplier shall make available to Purchaser for retrieval all Purchaser data in the XaaS/Cloud Service in an agreed format and for a period of time mutually agreed beforehand with the Purchaser.

As per sections D.2 and G.4, only encrypted connections shall be used for Purchaser retrieval of data unless exception agreed in writing by Purchaser.

At the end of the data reversibility period, the Supplier shall destroy all Purchaser environments and Purchaser data in the XaaS/Cloud Service in a manner designed to ensure that they cannot be accessed or read.

The Supplier shall provide the Purchaser with a certification of destruction.

H ACCESS CONTROL OF XAAS/CLOUD SERVICES

H.1 Physical security

The Supplier shall provide physically secured facilities for both production cloud infrastructure and locations for remote operations.

Controls shall include at least:

− physical access requires authorization and is monitored;

− everyone must visibly wear official identification while onsite;

− visitors must sign a visitor's register and be escorted and/or observed when on the premises; and

− possession of keys/access cards and the ability to access the locations is monitored. Staff leaving Supplier employment must return keys/cards.

H.2 System access control and password management

The Supplier shall control the Service systems by restricting access to only authorized personnel.

The Supplier shall enforce password policies on infrastructure components and cloud management systems used to operate the Supplier Service environment. The Supplier shall protect passwords using secure mechanisms such as digital vault.

The Supplier shall implement system access control, and accounting designed to ensure that only approved operations and support employees have access to the systems. System access control shall include system authentication, authorization, access approval, provisioning, and revocation for employees and any other Supplier-defined 'users'.

H.3 Review of access rights

Network and operating system accounts for Supplier employees shall be reviewed regularly to ensure appropriate employee access levels.

In the event of Supplier employee´s leaving the contractual project, the Supplier shall take prompt actions to terminate network, telephony, and physical access for such former employees.

H.4 Security Gateway

The Supplier shall utilize security gateways (e.g. firewalls, routers, proxies, reverse proxies) to control access between the internet and Supplier Services by allowing only authorized traffic.

Supplier managed security gateways shall be deployed to perform packet inspection with security policies configured to filter packets based on protocol, port, source, and destination IP address, as appropriate, in order to identify authorized sources, destinations, and traffic types.

H.5 Anti-malware controls

The Supplier shall employ anti-malware software to scan uploaded files. Malware definitions shall be updated at least daily.

H.6 Encryption and remote connections to XaaS/Cloud Services

For Purchaser access to and use of a XaaS/Cloud Service, only encrypted connections must be used unless exception agreed in writing by Purchaser.

The Supplier shall ensure that only authenticated and encrypted connections are used for Third Parties acting on behalf of the Supplier accessing remotely Purchaser data processed and/or stored in a XaaS/Cloud Service.

In all cases, the latest available browsers must be supported for connecting to Xaas/Cloud Services.

I OPERATIONS OF XAAS/CLOUD SERVICES

I.1 Penetration tests

The Supplier shall assess the security of the XaaS/Cloud Service using penetration tests at least on a yearly basis. The report and mitigation plan of such tests shall be shared with the Purchaser.

Notwithstanding the above, the Supplier shall allow the Purchaser to make XaaS/Cloud Service penetration tests on its production environment.

I.2 Production data and environments

The Supplier shall not use production data for testing activities.

The Supplier shall separate development, testing and production environments (e.g. networks, data, applications, etc.).

I.3 Disaster recovery plan

The Supplier shall set up and maintain a disaster recovery plan and ensure that it is tested at regular intervals.

The report including the results of such tests shall be shared with the Purchaser upon request.

Backups will be securely deleted by the Supplier upon disposal.

I.4 Security-related maintenance

For any security patch that the Supplier intends to deploy on the Xaas/Cloud Service, the Supplier shall apply and test the security patch on a testing environment. Only after successful completion of testing on such environment, the Supplier will deploy the patch on the production environment.

I.5 Third Party services

The Supplier shall inform the Purchaser if Third Party services (e.g. data center services) are involved or planned to be involved in the provision of the Service.

I.6 Relocation of data

The Supplier shall inform the Purchaser if Purchaser data is relocated to another data center (including backups) than initially agreed in the Agreement.

J ACCESS TO AND USE OF PURCHASER SYSTEMS AND RESOURCES

This section will be applicable only if the Purchaser grants the Supplier access to and use of Purchaser systems for the performance of the Agreement.

J.1 Physical

If Purchaser provides access and/or interconnection equipment installed on Supplier premises, the Supplier shall ensure that:

- physical access control is applied to the technical area where such equipment is located; and

- physical access to such equipment is limited to those who need to access the equipment for the performance of the Agreement and duly authorised by the Supplier.

J.2 Purchaser Systems

The Supplier shall:

- access and use Purchaser's systems only to provide the Deliverables;

- ensure that access and data transfer are not used to perform an attack (e.g. for data transfer, check for malware);

- comply with the means of access and rules defined by the Purchaser and provided to the Supplier beforehand (e.g. respect network addresses assigned by Purchaser, respect Purchaser responsive times for Purchaser management Resources, ...);

- ensure that anybody acting on behalf of the Supplier who needs to use the Purchaser systems is duly authorised by the Supplier and identification information has been provided to the Purchaser; and

- ensure that only duly authorised Supplier Resources are connected with the Purchaser systems.

J.3 Supplier Resources

The Supplier shall access the Purchaser network only using DTAG's remote access solution.

J.4 Purchaser systems and applications

If the Purchaser provides accounts to the Supplier, the Supplier shall:

- promptly notify the Purchaser when an account is no longer required; and

- ensure that accounts provided for server communications are used only for that purpose.

J.5 Management of Purchaser Resources

If the Purchaser provides physical Resources (software, hardware, computers, USB stick, badge, tablet, smartphone, access or interconnection equipment…) to the Supplier, the Supplier shall keep track of such Resources. Upon termination of the Agreement, the Supplier shall return Purchaser Resources still in his possession.

K PROFESSIONALS AND SECURITY

K.1 Awareness training and education

The Supplier shall ensure that his employees and any Third Parties appointed to provide the Deliverables:

- possess appropriate security skills (e.g. to manage security incidents); and

- are familiar with the content and the implementation of applicable security rules.

K.2 Purchaser specific security rules

If the Purchaser provides specific security rules for performing the Professional Services, the Supplier shall ensure that his employees and any appointed Third Parties are informed of such rules before the start of any tasks.

K.3 Subcontractors

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

K.4 Handling of sensitive Deliverables

Upon request of the Purchaser and agreed in the NPA, the Supplier shall commit to use only security checked personnel, i.e. screened by national authorities, for handling of sensitive Deliverables prior to deployment in the Purchaser's Network, as well as for maintenance of sensitive Deliverables during the whole operational phase.

K.5 Handling of Purchaser's data

The Supplier shall ensure that his employees and any Third Parties with access to data of the Purchaser shall have passed a security background check (e.g. criminal record check).

L DISTRIBUTION OF SOFTWARE UPDATES

NOTE: this section is only applicable to Customer Equipment Deliverables.

The availability of a software update by the Supplier within the support period (see F.9) of a Deliverable shall be free of additional charge for the Purchaser, as well as for the end user.

The Supplier shall promptly deliver a software update (such as a whole firmware image file, a single application update, etc) using any mechanism as set our in the Agreement as soon as a security Vulnerability in the software of a Deliverable is identified and according to section F.4.

The Supplier shall respect the process agreed with the Purchaser before distributing any new software update.

The distribution of the security fix shall use state-of-the-art technical approach (device firmware upgrades, app updates through app stores, ….) in order to fix the vulnerability in the field on all vulnerable devices.

In connection with F.4, for Deliverables running an Android operating system, the Supplier's must provide regular updates maintaining the Security Patch Level (SPL) of the Deliverables in less than 90 (ninety) days (or any shorter period requested for the certification of such Deliverables) during the whole Lifecycle of the product.

DEFINITIONS AND ABBREVIATIONS

Agreement	means any contract signed by BuyIn, DTAG with the Supplier and containing the reference to this ISA.
Assets	encompass primary and supporting assets as defined in ISO/IEC 27005.
Audit Report	means the document presenting the results of the audit conducted at the Deliverable by the audit team, as defined in GSMA *"FS.13 - Network Equipment Security Assurance Scheme – Overview"*
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/.
Defect	means any deviation of the actual quality of the Deliverable from the contractually intended quality, e.g. default, non-compliance of the Deliverables with their corresponding specification or their failure to perform in accordance with related documentation.
Deliverables	mean any equipment, product and/or service ordered on the main Agreement including all main- and ancillary obligations.
Evaluation Report	means documented assessment produced by a NESAS Security Test Laboratory of the level of compliance of a Deliverable with the relevant 3GPP defined Security Assurance Specification; as defined in GSMA *"FS.13 - Network Equipment Security Assurance Scheme – Overview"*
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).
Internet of Things	means any connected devices or equipment for internet of things
Lifecycle	means period including warranty period, support period and any extended support period of a product.
NPA	means a contract concluded by an Affiliated Company of DTAG under a Frame Agreement of BuyIn, DTAG concluded by BuyIn. NPA corresponds with the terms "Implementation Contract", "Project Specific Agreement" and "Project Agreement": any provision using the term "NPA" shall apply to those kinds of agreements as well.
Official Fix	means that a complete Supplier solution is available to fix a Vulnerability, either by means of an official patch or an upgrade.
Order	means a purchase order issued by the Purchaser. "Order" corresponds with the term "Purchase Order" in Agreements concluded by DTAG and its Affiliated Companies. Any provision using the term "Order" shall apply to "Purchase Order" in the same way.
Purchaser	means the DTAG Affiliated Company as party to the NPA or Order. "Purchaser" corresponds with the term "Ordering Party" in Agreements concluded by DTAG and its Affiliated Companies. Any provision set out for the Purchaser in this ISA shall apply to "Ordering Party" in the same way.
Purchaser Network	means the network managed by the Purchaser and all related Purchaser Network access infrastructures necessary to ensure the communications between each party Resources.
Purchaser Resources	means hardware, software, services belonging to the Purchaser and used for the purpose of providing the Deliverables.
Software Bill of Materials (SBoM)	means, as defined in ISO/IEC 27036, an inventory of software components, sub-components and dependencies with associated information
Software Result	means any software that is: (i) primarily based on and/or directed to the DTAG Requirements and/or Specifications provided by or exclusively for Purchaser, and/ or (ii) developed or implemented by Supplier under this Agreement (and/or any subsequent amendments) and/or any TSA and/or NPA and/or any Order, and which is not a background; which may or may not be protected by intellectual property rights, as well as any product or process resulting from it.
Statement of Compliance	means an exhibit of Agreement with detailed technical security requirements on Deliverables.
Statement of Work (SoW)	means a document defining project-specific activities, deliverables and timelines for the Supplier providing Deliverables and/ or Services to the Purchaser.
Supplier Resources	means hardware, software belonging to and/or under liability of Supplier and used for the purpose of providing the Deliverables.

Support Period	mean the period of times on which the Supplier is committed to provide support on the Deliverable, including security fixing. This Support Period shall not be shorter than the period mandated by applicable legislation or as agreed in the Agreement, whichever is longer.
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.
XaaS	means anything delivered to users as a service including SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) or similar.
Zero-Day	means an undisclosed vulnerability that hackers can exploit to adversely affect Deliverables. It is known as a "zero-day" (or "zero-hour" or "0-day" or "day zero") because it is not publicly reported or announced before becoming active, leaving the Supplier with zero days in which to create patches or advise workarounds to mitigate its actions.

- end of document -