Annex IS - Information Security
Version 3.1

1 APPLICABILITY

This **Annex Information Security** ("Annex IS") defines the Information Security requirements and corresponding rights and obligations of the Principal (hereafter for the purpose of this **Annex IS** referred to as **"Customer"**) and the Contractor (hereafter for the purpose of this Annex IS referred to as **"Supplier"**). The acronym "DBG" refers to Deutsche Börse Group, a group of companies comprised of Deutsche Börse AG, 60485 Frankfurt and its Affiliates- "Affiliate" means any person that, directly or indirectly, controls, is controlled by or is under common control with such Party; the term "control" means the possession of (i) 50% or more of the voting rights in the general meeting of a person or (ii) the power, directly or indirectly, whether by contract or ownership, to direct or cause the direction of the management and affairs of a person, including investment decisions.

2 CONTRACTUAL TERMS

Unless explicitly provided otherwise in this **Annex IS**, all terms of the Agreement agreed between the Customer and the Supplier (mutually the "Parties") remain unaffected. In case of any conflicts between the provisions of the Annex IS and those of the Agreement, the provisions of Annex IS shall prevail (to the extent permitted by applicable law and regulation).

This Annex IS defines Information Security requirements depending on the respective service or product type. The Information Security provisions can vary depending on the classification of the relevant information. The classification can be obtained from DBG.

Any deviation from this Annex IS must be made in writing and reference to the modified requirement or provision.

2.1 Information Classification and Handling Information with a major or critical classification

The Customer classifies all its information assets using a classification scheme which is based on the possible impact on the four security objectives: integrity, availability, authenticity, and confidentiality.

There are four information classifications:

- Critical
- Major
- Minor

- Negligible

For all classifications the same Information Security requirements apply. However, major, and critical information require a higher level of security which will be achieved by implementing additional security controls. These controls are described in chapter 4.

The highest rating in any of the four security objectives determines the overall classification of an information.

2.2 State of the Art Technology

Supplier shall provide its services using State of the Art technology and organizational measures, i.e. Supplier shall take all necessary measures in accordance with best practice standards like ISO/IEC 27001. 'State of the Art' is the process, equipment, or mode of operation available in the trade in goods and services which can most effectively ensure the security objectives. Supplier shall determine the State of the Art pursuant to the "Guideline State of the art Technical and organizational measures" 2021 released by European Union Agency for Cybersecurity (enisa) together with TeleTrusT – IT Security Association Germany as amended from time to time.

3 HUMAN RESOURCES SECURITY REQUIREMENTS

The Supplier shall ensure that its employees and contractors are aware of Information Security threats and concerns, understand their responsibilities in the topic of Information Security and are suitable for the roles for which they were assigned to. They shall be aware of and fulfil their explained or delegated Information Security responsibilities, including the confidentiality obligations hereunder, during their employment and after the termination of the employment relation.

Supplier shall perform appropriate background checks to verify the reliability of its personnel taking into account Information Security relevant aspects, based on the risk profile of the position e.g. by inspection of employee's police clearance certificates. All employment agreements for Supplier's personnel shall be made in writing and include strict confidentiality obligations during and after the employment. Supplier shall ensure, that Supplier's personnel is adequately trained regarding Information Security and security awareness.

4 INFORMATION SECURITY REQUIREMENTS

The Supplier shall develop, maintain, and keep a security concept that complies with the State of Art describing Supplier's product's and services' compliance with the Security requirements below and

- The Supplier shall fill out and provide the self-assessment questionnaire to the Customer once per year. The Supplier represents and warrants that the information provided in the self-assessment questionnaire is accurate and actual.

- The Supplier shall appoint a member of its personnel (e.g. the "**Information Security Officer**") to coordinate and manage information and technology security issues and processes related to Supplier's engagement with the Customer. This employee shall act as primary contact person to the Customer for any Information Security related matters.

- The Supplier shall ensure that its IT systems and IT processes adequately and effectively protect the integrity, availability, authenticity, and confidentiality of Customer data.

4.1 Information Security Compliance

The Supplier shall analyze and document all relevant legislative statutory, regulatory and contractual duties along with his organization's approach to avoid breaches of obligations related to Information Security. To fulfil the identified requirements, Supplier shall predefine and document the specific controls and responsibilities for each requirement.

The Supplier shall ensure that information assets are effectively protected against loss, destruction, falsification, unauthorized access, and unauthorized release.

As one element of the measures to meet these information assets safeguarding objectives, the Supplier shall implement, maintain, and follow effective guidelines on the retention, storage, handling and disposal of records and information.

4.2 Information Security Policies

The Supplier shall implement and maintain effective policies safeguarding Information Security that are approved by management and shall communicate these policies to employees and relevant third parties. These policies shall contain requirements concerning the definition of Information Security objectives and principles to guide all activities relating to Information Security including the addressing of identified threats. The Supplier shall review and update the Information Security policies periodically and as required to address actual developments.

Based on the Information Security policies, the Supplier shall maintain specific, state of the art Information Security guidelines and Information Security processes.

The Supplier shall review the compliance of its information processing and procedures as well as information systems with the appropriate security policies, standards, and any other security requirements on a regular basis.

4.3 Information Security Management System

The Supplier shall establish and maintain an Information Security Management System (ISMS) based on best practice international standards, e.g. ISO 270xx, including ISMS governance structure, roles & responsibilities, resources, policies, standards, and processes.

The Supplier shall establish an approach for monitoring and measurement of the Information Security Management System and annually review this approach, including control domain design and operational effectiveness. Supplier shall promptly rectify any shortcomings identified.

The Supplier shall define and integrate an Information Security risk management framework in its overall ISMS and align it with its risk management function.

The Supplier shall ensure its Information Security is embedded in the business continuity management system and processes.

Prior to commencement of the service, the supplier shall inform the Customer in writing of the locations at which it stores Customer data or has Customer data stored in the course of providing the service and shall notify the Customer of any intended and completed change of the storage or processing locations. Agreements between Supplier and Customer on data location remain unaffected.

4.4 Asset Management

The Supplier shall establish and maintain effective controls to protect its assets associated with information and information processing facilities over its lifecycle. The lifecycle of the information generally includes creation, processing, storage, transmission, deletion, and destruction stages.

The Supplier shall maintain an accurate and current inventory of assets that manages information based on their classification and establish accountability by awarding asset responsibility.

The Supplier shall maintain rules for the classification of assets based on legal requirements, value, criticality, business impact and vulnerability to unauthorised disclosure or modification.

The supplier shall appropriately protect Supplier's assets by implementing appropriate security controls based on the criticality of the respective assets derived from information classification and security requirements.

The Supplier shall maintain procedures for the acceptable use of information and assets associated with information and information processing facilities in accordance with its information classification scheme.

4.5 Access Control

The Supplier shall have established and documented an access control policy on business and Information Security requirements that includes appropriate access control rules (logical and physical), access rights and restrictions for specific user roles towards their assets reflecting the associated Information Security risks.

The Supplier shall

- grant access to information, information processing facilities, network and network services only on a need-to-know basis as required for the provision of its services and after proper authorization;
- ensure effective authentication and authorized user access (including privileged access), e.g. by segregation of access control roles, access requests, access authorizations, access administrations;
- determine a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services;
- ensure that access rights of all employees and third parties to information and information processing facilities are removed or adequately adjusted upon change of role, responsibility, employment or contract as well as termination of employment, or contract that required access to the information or information processing facilities.
- ensure that users access rights are reviewed and adequately adapted at regular intervals, which shall not be longer than six months for privileged user accounts and twelve months for all other user accounts;
- prevent unauthorized access to information, application system functions, systems, networks, services and applications;
- ensure that password management systems and password quality and complexity comply with generally accepted standards or the state of the art.

Regarding privileged access or access to information classified as major or critical, Supplier shall

- ensure that in addition access to information classified as major or critical is secured using two-factor authentication;
- register and maintain all privileged access accounts in accordance with the information asset inventory;
- shall control activities of privileged user accounts and the use of network services handling information classified as major or critical, and continuously use a monitoring and logging system that protocols executed actions, user ID, time of information access and information modified. It is imperative that the protocols produced by the monitoring and logging system cannot be altered. Legitimate and prohibited behavior of privileged users shall be defined in applicable policies.

The Supplier shall establish and maintain effective rules, guidelines and measures to restrict and control access to program source code and associated items (such as designs, specifications, verification plans and validation plans).

4.6 Physical and Environmental Security

The Supplier shall define and use security perimeters to protect areas that contain information and information processing facilities relevant for Supplier's services or goods. These security perimeters shall include at least, but are not limited to, effective controls against physical penetration by malicious or unauthorised persons, damages of relevant Supplier infrastructure, unauthorised modification, external and environmental threats, and interruption of Supplier organization's operations.

Furthermore, the Supplier shall effectively protect infrastructure that holds and transmits data and hardware such as power and telecommunications cabling as well as network cabling carrying data or supporting information services from interception, physical tampering, interference, and damages.

The Supplier shall apply security controls to equipment, information, and software, that can be taken off-site, taking into account the different risks of working outside the organization's premises.

Supplier shall implement the following guidelines for the protection of equipment, information and software that can be taken off-site:

- equipment, information or software may not be taken off-site without prior authorization;

- controls for off-premises locations, such as home-working, teleworking and temporary sites shall be determined by a risk assessment and suitable controls applied as appropriate;

- if equipment, that can be taken off-site is transferred among different individuals or external parties, a log must be maintained that defines the chain of custody for the equipment including names and organizations of such individuals or external parties, who are responsible for the equipment as minimal requirement.

The Supplier shall verify all items of equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten (5220.22-M-Standard of the US DoD, VSITR-Standard of the BSI, Bruce-Schneier-Algorithm or similar) prior to disposal or re-use.

The supplier shall adopt a clean desk policy for papers and removable storage media and a clear screen policy for information processing facilities.

4.7 Operations Security

The Supplier shall establish and document operating procedures for operational activities associated with information processing and communication facilities.

The use of resources shall be monitored, adjusted and projections made of future capacity requirements to ensure the required system performance. Changes to IT assets, software packages, systems within the development lifecycle, business processes, information processing facilities and systems that affect Information Security shall be monitored and controlled through a formal change control process. For the development, customization or modification of software, the Supplier shall ensure development, testing, and production environments are separated.

The Supplier shall implement and maintain rules and procedures for the installation of software on operational systems as well as operating procedures for all applications. Furthermore, there must be security documentation that details and proves the implementation of relevant security controls, which were aligned with the Supplier's Information Security.

The Supplier shall implement and maintain controls that protect information involved in application services passing over public networks against fraudulent activity and unauthorized disclosure and modification.

The Supplier shall use effective measures including detection, prevention, and recovery controls, to protect its and Customer's infrastructure against malware. Supplier personnel shall be adequately trained to be aware of the threats of

malware and measures and methods to prevent and defend against such threats.

If the Supplier operates its own systems or offers any form of software related service, the Supplier shall have established a patch management process and patch their systems on a regular basis.

The Supplier shall have established and implemented a backup policy which shall include requirements for the retention and protection of information. Backups shall be designed according to business requirements and risk levels relating to the unavailability of information.

The Supplier shall have established and implemented processes for the recording, storing, and reviewing of event logs of user activities, exceptions, faults, and Information Security events. System administrator and system operator activities shall be logged, and the logs shall be protected and regularly reviewed.

The Supplier shall have implemented and maintain processes for identifying and detecting vulnerabilities, especially on systems critical for the provisions of Supplier's services or those processing or storing information classified as major or critical. The Supplier shall continuously monitor and assess information about technical vulnerabilities of its information systems and take appropriate measures to address the associated risks. Any vulnerability is a weakness in security protection and must be dealt with effectively and efficiently when risk levels are unacceptable for the provisions of Supplier's services or pose a risk to the Information Security of the Customer. The Supplier shall implement hardening measures and change configurations according to the identified risks.

4.8 Communications Security

The Supplier shall maintain and implement effective controls to ensure protection of information networks and its supporting IT assets, and to maintain the end-to-end security of information transferred within and outside of its organization. Security mechanisms, service levels and management requirements of all network services shall be identified and included in network service agreements, whether these services are provided in-house or outsourced.

The Supplier shall have established and implemented policies, procedures and controls for the transfer of information, especially with the aim of protecting Information involved in electronic messaging, and shall secure its communication by utilizing an effective Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS).

Protection of data in transit (leaving DBG's internal network): Supplier shall protect data in transit depending on its classification and the following rules:

- if data communicated to recipients outside of DBG's internal network, cryptographic measures must be used for data classified as "critical" or "major" with respect to confidentiality and/or integrity and/or authenticity or when the data is labelled "strictly confidential" or "confidential";

- if data communicated to recipients outside of DBG's internal network, cryptographic measures should be used for data classified as "minor" with respect to confidentiality and/or integrity and/or authenticity or when the data is labelled "internal".

Protection of data at rest (stored outside of DBG's internal infrastructure or approved datacenters): Supplier shall protect Data at rest stored outside of DBG's internal infrastructure or approved datacenters on its classification and the following rules. For data classified as "critical", "major" or "minor" with respect to confidentiality and/or integrity and/or authenticity and where the data is labelled "strictly confidential", "confidential" or "internal" Supplier shall use cryptographic measures to protect the data:

- if data is classified as "minor", "major" or "critical" or when data is labelled "internal", "confidential" or "strictly confidential", it must be encrypted using cryptographic measures in line with BSI technical guidelines to preserve its confidentiality (the data is sent in encrypted form to external servers);

- Furthermore, cryptographic measures in line with BSI technical guidelines must be used to ensure that only authorized persons access the systems to preserve integrity and authenticity.

For the information exchange between the Supplier and the Customer, Supplier shall implement and maintain the following controls:

- responsibilities and accountabilities for controlling data transmission as well as in the event of Information Security incidents;

- procedures to ensure traceability and non-repudiation.

- any special controls that protect critical information in transit, meaning encryption.

4.9 System Acquisition, Development and Maintenance

The Supplier shall maintain an inventory of all relevant applications and IT systems. All applications and IT systems must be reviewed for compliance with Information Security requirements.

If the Supplier develops or updates software, there must be a defined and documented process for review of information system (including the operating platform) changes to ensure that Information Security controls have not been compromised. Modifications to software must be limited to necessary changes and all changes have to be reviewed and for both a technical and user acceptance test shall be conducted. The Supplier shall ensure that test data is selected carefully, protected, and controlled. Any use of the Customer's productive data must be pre-authorized, logged and monitored by the Customer.

For IAAS / PAAS / SAAS providers, the following requirements must be met:

The Supplier shall perform yearly tests for the authentication of security breaches ("**penetration test**"). The penetration test results shall be made available to the Customer on demand. The specific test type must be predefined beforehand. The scope of the penetration test shall at least contain significant weakness categories as minimum requirements.

The Customer has the right to perform security penetration testing to assess the effectiveness of implemented security measures and processes.

The Supplier shall establish protection against Distributed Denial of Service Attacks ("**DDos Attack**").

The Supplier shall offer interfaces for Security Information and Event Management integration, where applicable.

4.10 Information Security Incident Management

The Supplier shall have established and implemented management responsibilities and procedures for an effective and orderly response to Information Security incidents so he can respond accordingly.

The Supplier notifies the Customer promptly but in no case within more than 72 hours of any security incident in the information processing environment in relation to the Information handled and / or services provided by the Supplier to the Customer. The notification needs to be sent to: cert@deutsche-boerse.com.

The supplier will use the knowledge gained from analysing and resolving information security incidents to reduce likelihood and impact of future incidents.

5 REQUIREMENTS FOR THE SECURE SOFTWARE DEVELOPMENT LIFECYCLE

The Supplier shall implement and maintain policies, guidelines, and procedures for the development of software and systems.

The Supplier shall have developed controls to ensure:

- all applied development methodologies must implement security modules to secure all stages of a software development lifecycle;
- the security of the development environment;
- requirements exist for the security in the software development lifecycle including security in the software development methodology and secure coding guidelines for each programming language used;
- a proper software version control shall be in effect to minimize the risk of accidental deployment of incorrect or outdated software versions;
- principles for engineering secure systems that are maintained and applied to any information system implementation;
- secure development environments for system development and integration efforts that cover the entire system development lifecycle;
- secure procedures for decommissioning code are defined and implemented.

When operating platforms are changed, the Supplier shall ensure business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.

In line with the state of the art, the Supplier shall conduct regularly, but at least once before the release of the software, source code scans with regards to potential security weaknesses. The Supplier shall confirm in written form that source code scans were conducted and provide the results to the Customer.

The Supplier shall provide any source code to the Customer for the Customer to conduct source code reviews and analysis, e.g. vulnerabilities scanning and penetration testing.

Supplier shall not store or process uncompiled source code in testing environments. If source code needs to be tested, it must be compiled into a binary data type, commonly known as byte code or object code.

6 REQUIREMENTS FOR CLOUD SERVICES

The Supplier shall define and maintain documented operating procedures regarding critical operations where failure can cause unrecoverable damage to assets in the cloud-computing environment.

The Supplier shall implement and maintain technical measures to ensure that all changes to the cloud-computing environment correspond directly to a documented change request. Prior to implementation in production, the change and used business-critical data must be approved by the Customer or the change must be made in accordance with a Service Level Agreement. The Supplier shall provide to Customer technical capabilities allowing detailed security monitoring and near-time alerting.

The Supplier shall ensure that configuration reviews of network environments and virtual instances will be conducted at least annually.

The Supplier shall ensure that DBG data is always stored and transferred using cryptographic measures protecting at least integrity, authenticity and confidentiality of the DBG data.

DBG data stored in cloud services should be protected using Cryptographic Keys generated On-Premise and maintained by Suppliers staff (Bring Your Own Key).

The Supplier shall define, identify, and assign to members of its personnel at least the following roles:

- an information owner for all cloud infrastructure, who is responsible for the corresponding information;
- a security point of contact, who is in charge of interfacing with the Customer's Information Security personnel;
- a cloud infrastructure owner, who is in charge of managing the lifecycle of all devices deployed within the Cloud and of implementing standards for all deployments;
- a Head of IT, acting as single point of contact interfacing with senior management of the Customer, in case of issues that require escalation;
- IT Operators, who manage the devices of the Information Owner deployed within the Cloud.

The roles must clearly describe the level of clearance in relation to the level of privileged accesses.

7 CHANGE OF INTERNAL COMPANY AFFAIRS

The Supplier shall inform the Customer when changes concerning the Information Security Officer and any official contact person within the Supplier's engagement with the Customer, occur.

The Supplier shall inform the Customer, if there is a significant change in any of the controls it has in place in order to comply with the Information Security requirements defined by the Customer.

8 CONFIDENTIALITY

a) Confidential Information means all business, technical, proprietary, trade secret or other information disclosed or made available by the Customer or its Representatives ("Disclosing Party") to the Supplier or its Representatives ("Receiving Party") before or after the date of this Annex IS, including without limitation information relating to the Disclosing Party's customers, products, services, operations, technologies, processes, methodologies, data, knowledge, know-how, software, algorithms, planned or existing computer systems and systems architecture, research and development, marketing plans and financial matters. "Representatives" means a Party's Affiliates as well as the directors, officers, employees, legal counsel, accountants, auditors and other representatives and advisors (including, without limitation, financial advisors, and consultants) of a Party or a Party's Affiliates. Customer Penetration test results shall not constitute Confidential Information of Supplier and may be shared with DBG entities and published in an IT security industry standard responsible disclosure procedure.

b) Confidential Information shall not include information that

- at the time of disclosure by the Disclosing Party is publicly known;
- following disclosure by the Disclosing Party becomes publicly known other than as a result of unauthorized disclosure by the Receiving Party or the Receiving Party's Representatives in breach of this Annex IS;
- prior to the time of disclosure by the Disclosing Party is known by or is in the possession of the Receiving Party or one or more of its Affiliates;
- becomes available to the Receiving Party or one or more of its Affiliates from a third party which is not reasonably known by the Receiving Party or its respective Affiliate(s) to be prohibited by a contractual, legal, fiduciary or other obligation to the Disclosing Party from disclosing the information to the Receiving Party or its respective Affiliates(s); or

- is lawfully and independently developed, discovered, or arrived at by the Receiving Party or any of its Representatives without use of Confidential Information

c) The Receiving Party shall bear the burden of proof for establishing one of the foregoing exceptions.

d) The Receiving Party shall keep the Confidential Information confidential and shall not disclose or reveal any Confidential Information to any third party without the prior written consent of the Disclosing Party. The Receiving Party may, however, disclose Confidential Information to its Representatives if they have a strict need to know such information for the performance of the contracts and the Receiving Party has procured compliance by its Representatives with confidentiality obligations protecting the Confidential Information, that are equivalent to the terms of this Section 8. This shall always be deemed given for any disclosure of Confidential Information to DBG entities. The Receiving Party agrees to be responsible for all use of Confidential Information by its Representatives and shall be liable for any breach of the confidentiality provisions caused, directly or indirectly, by its Representatives.

e) The Receiving Party and its Representatives may not use the Confidential Information for a purpose other than the performance of its obligations or the exercise of its rights under this Annex IS.

f) The Receiving Party shall use all reasonable efforts to keep the Confidential Information of the Disclosing Party in confidence and to safeguard the Confidential Information. In so doing, the Receiving Party shall take at least the same precautions which it would take to safeguard its own similarly valued proprietary and confidential information but shall in no event take less than commercially reasonable precautions. The Receiving Party shall take all measures (including court proceedings) to restrain or prevent any breach of the confidentiality obligations pursuant to this Annex IS by its Representatives.

g) The Receiving Party shall not disclose to any third party any information that is protected by banking secrecy or stock exchange secrecy, whether such secrecy is established by law, by contract, or otherwise. The Receiving Party will impose on Receiving Party's personnel and on any commissioned sub-contractor an obligation to comply with banking secrecy and stock exchange secrecy. Upon Customer's request, the Supplier will demonstrate its corresponding measures.

h) The Receiving Party or its Representatives may disclose Confidential Information to the extent

- required by any applicable law or regulation (which shall, for the avoidance of doubt, include the requirement to inform the public of inside information under the European Market Abuse Regulation – MAR);

- requested by any binding order or directive of any court, governmental or regulatory authority having competent jurisdiction over the Receiving Party; or

- required pursuant to the rules and regulations of any stock exchange on which the securities of the Receiving Party or any of its Affiliates are listed;

provided, however, that the Receiving Party, unless prohibited by law (e.g. by the requirement to inform the public of inside information under MAR), regulation or court or regulatory order to do so, (i) promptly notifies the Disclosing Party, orally or in writing, upon receipt of any request for disclosure of its Confidential Information; and (ii) reasonably cooperates with the Disclosing Party so as to provide the Disclosing Party with a reasonable opportunity, at its own expense, to (1) contest and assist in opposing any requirement of disclosure of its Confidential Information; (2) seek judicial protection against the disclosure; and (3) have such required disclosure be made under a protective order.

i) Upon receipt of a written request from the Disclosing Party at any time, the Receiving Party shall, and shall procure that its Representatives shall, promptly either (a) return to the Disclosing Party all documents or materials (including computer media) or such parts thereof containing or reflecting any Confidential Information in the possession or control of the Receiving Party or its Representatives or (b) permanently destroy, erase or delete all the Confidential Information in the possession or control of the Receiving Party or its Representatives, in particular, but not limited to, from any computer, word processor, mobile telecommunication device or similar device into which it was stored or programmed, and provide to the Disclosing Party written confirmation of such destruction, erasure or deletion.

j) The Receiving Party may, however, retain such Confidential Information which it is required to retain according to any applicable law or regulation, or which has been created pursuant to automatic archiving and back-up procedures. Also, for the avoidance of doubt, the General Legal Counsel of the Receiving Party may retain one complete set of Confidential Information solely for legal purposes. In all cases covered by this Section any retained Confidential Information shall be retained on the terms of confidentiality set out in this Annex IS, with the exception that it may be used as deemed necessary in litigation proceedings between the Parties or with third parties in connection with the Project and where such disclosure is necessary for the outcome of the proceedings.

k) Each Party acknowledges that neither the destruction or return, nor the deletion of any Confidential Information will release it from the obligations contained in this Annex IS.

l) The Receiving Party acknowledges that the Confidential Information is of unique character and agrees that any direct or indirect breach of this Annex IS will irreparably harm the Disclosing Party in a way that recovery of damages could not adequately compensate. Therefore, in the event of the Receiving Party's direct or indirect breach of confidentiality or non-disclosure, the Disclosing Party is entitled to the immediate termination of this Annex IS and the contracts under this business relationship for cause and to an injunction or other equitable relief as may be deemed proper by a Court.

m) This Section 8 and the confidentiality obligations hereunder shall survive the termination or expiration of the Annex IS.

9 SUB-CONTRACTING

Supplier may only sub-contract the performance of any of the Services or parts of them under this business relationship to a third party upon prior written consent of the Customer, which will not be unreasonably withheld. Supplier remains liable for the sub-contracted services or processes.

For each intervention from the sub-contractor on the Customer´s production system a formal agreement is mandatory.

The Supplier shall ensure that the sub-contractors (including all sub-contractors within the delivery chain) fulfil and comply with the security requirements as described in this Annex IS. The Supplier shall monitor the implementation of the required Information Security requirements on a regular basis. The Customer's right to audit as referred in chapter 10 also applies to the Supplier's sub-contractors.

10 RIGHT TO AUDIT

Upon Customer's written request, the Supplier grants the Customer, its internal auditing department, external auditors engaged by the Customer and supervisory authorities exercising their supervisory powers over Customer and third parties assigned by such supervisory authorities in such context, during the term of the Annex IS and for 3 years thereafter, an unrestricted right to audit the Supplier and its sub-contractors, including without limitations full access to all relevant business premises, including the full range of relevant devices, systems, networks, information, documents and data used for providing, or related to the outsourced function, including related financial audit reports of

Supplier´s internal control functions, information, personnel and the service provider's external auditors in relations to information handled.

The Supplier will provide any information and documents required by Customer in such audit. The Supplier shall release all employees required by the Customer in the course of an audit from their confidentiality obligations. The Customer will seek to reasonably minimize interruptions of Supplier´s regular business activities.

Customer is entitled to conduct security penetration testing on infrastructure used by Supplier to provide its services or produce its goods, to assess the effectiveness of implemented cyber and internal ICT security measures and processes, can be conducted if relevant for services/criticality.

The Supplier shall perform, and provide to Customer in writing, self-assessments regarding its cyber resilience on Customer request.

11 MONITORING AND REPORTING OBLIGATIONS

**** For outsourcing partners: Mandatory. Key Risk Indicators (KRI) and reporting period will be adjusted depending on risks and the product / service.*

**** For all other third party providers: Optional. Key Risk Indicators (KRI) and reporting period will be adjusted depending on risks and the product / service.*

Service Level Targets (SLT) and Key Risk Indicators (KRI) for Information Security are agreed upon between the Parties in the Service Level Agreement listed below.

The reporting of Key Risk Indicators (KRI) are mandatory for outsourcing partners, while being optional for other third party providers. The specific KRI or / and KPI as well as reporting periods that are suggested below will be adjusted depending on the specific product / service provided by the Supplier and on risks.

KRI reports include, but are not limited to:

Monthly reports on Information Security Key Risk Indicators
(1) Number of security incidents, classified by severity category.
(2) Security threats and vulnerabilities, classified by severity category.

The Supplier shall notify the Customer promptly of any event that violates or may violate the Information Security objectives ("Security Incident") in Supplier's infrastructure used to provide services to the Customer. This includes any unauthorized disclosure, misappropriation or misuse of any Confidential Information. The Supplier shall provide an analysis of the effects and its mitigating actions.

The Supplier shall notify the Customer promptly of any changes implemented in the environment in relation to the Information handled and / or services provided by the Supplier to Customer used for the provision of services to Customer or for processing or storing Customer information. The Supplier shall provide an analysis of the effects of the changes and any defects that occurred during testing and implementation to Customer in writing.

Quarterly reports on Information Security Key Risk Indicators
(1) Percentage of vulnerability scans performed – The number of performed vulnerability scans as a percentage of the total systems requiring annual vulnerability scans.
(2) Duration from the identification of a security threat and / or security vulnerability to the implementation of a suitable remediating measures. Number of vulnerabilities exceeding due dates for remediating measures.
(3) Number of security tests and number of identified vulnerabilities, categorized by the severity classification.
(4) Number of identified vulnerabilities during security tests, classified by severity category.
(5) Any development that may have a material impact on the service provider's ability to effectively carry out its services or critical or important functions.

The Supplier shall identify risks associated with the confidentiality, integrity, authenticity, and availability of the information assets of the Customer and implement risk mitigating measures. In the case that any risk identified at the beginning of the Annex IS changes, the Supplier shall notify the Customer quarterly in an additional reporting.

Annual reports on Information Security Key Risk Indicators
(1) Percentage of changes considered emergency changes – The number of changes, or patches that are considered to be an emergency change as a percentage of changes in a year.
(2) Percentage of systems in use that are no longer supported of the software developer or vendor – The number of systems currently in use that are no longer supported by the software developer as a percentage of the total systems in use.

(3) Percentage of critical systems without up-to-date patches – The number of critical systems that do not currently have up-to-date patches installed and running as a percentage of total systems in use.
(4) Confirmation of source code scans – In case the Supplier develops software that processes the Customer's information a confirmation of any form that source code scans for vulnerabilities of the developed software were conducted including a confirmation that the vulnerabilities were closed.

The Supplier shall provide a written report on the current state of the implementation of the Information Security Controls defined by the Customer annually. The report shall include, at a minimum, a summary of all changes to controls and the control environment, and possible resulting risks and the remediating measures.

12 RECORD RETENTION REQUIREMENTS

The Supplier shall maintain all records that contain the Customer's information pertaining to the Service provided to Customer under this Annex IS, and if longer after termination of the business relationship, subject to applicable law or regulation. The Supplier further agrees to provide to the Customer, at its request, all relevant data (to the extent permitted by applicable law).

13 GLOSSARY

Attack	An attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
Authenticity	The property that an entity is what it claims to be.
Availability	The property of being accessible and usable on demand by an authorized entity.
Confidential Information	Confidential Information means all business, technical, proprietary, trade secret or other information disclosed or made available by the Customer or its Representatives ("Disclosing Party") to the Supplier or its Representatives ("Receiving Party") before or after the date of this Annex IS, including without limitation information relating to the Disclosing Party's customers, products, services, operations, technologies, processes, methodologies, data, knowledge,

	know-how, software, algorithms, planned or existing computer systems and systems architecture, research and development, marketing plans and financial matters.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Control	A measure that is modifying risk. Note 1: Controls include any process, policy, device, practice, or other actions which modify risk. Note 2: It is possible that controls not always exert the intended or assumed modifying effect.
Major / Critical Information	Information which has been classified as “major / critical” regarding at least one of the four security objectives confidentiality, integrity, authenticity or availability. The Information Owner defines the criticality of the information.
Deletion	A way of removing a file from a computer's file system and securely overwriting it.
Development Lifecycle	A process for planning, creating, testing, and deploying an information system.
Distributed Denial-of-Service Attack (DDoS Attack)	Distributed Denial-of-Service Attack (DDoS Attack) means a cyberattack with an attempt to make a machine or network resource unavailable to its intended users where incoming traffic flooding the victim originates from many different sources.
Governance of Information Security	The system by which an organization’s information security activities are directed and controlled.

Information asset	Information such as data or documents, and information processing facilities such as networks, systems and applications.
Information Processing Facilities	Any information processing system, service or infrastructure supporting business processes considering the physical location housing it.
Information Security	The preservation of confidentiality, integrity, availability, and authenticity of information.
Information Security Event	An identified occurrence of a system, service or network state indicating a possible breach of Information Security policy or failure of Controls, or a previously unknown situation that can be security relevant.
Information Security Incident	A single or a series of unwanted or unexpected Information Security events that have a significant probability of compromising business operations and threatening Information Security (e.g. attempt to gain unauthorized access to information).
Information Security Management System (ISMS)	System that defines the methodology, rules, procedures, measures, and control measures for protection of information in the organization pursuant to the ISO standard series ISO / IEC 270XX.
Integrity	The property of accuracy and completeness.
Non-Repudiation	The ability to prove the occurrence of a claimed event or action and its originating entities.
Patch	A set of changes to a computer program or its supporting data designed to update, fix, or improve it.
Penetration Test	Security assessment which aims to identify the security vulnerabilities on the target systems that can be exploited by attackers.

Policy	Intentions and direction of an organization, as formally expressed by its top management.
Source code	Human readable code written in a specific coding language.
Threat	A potential cause of an unwanted incident, which can result in harm to a system or organization.
Vulnerability	A weakness of an asset or control that can be exploited by one or more threats.