Table of Contents

1. CYBERSECURITY MEASURES

This Appendix sets forth CLIENT's cybersecurity measures applicable to the delivery of the goods and/or performance of the services (the "Goods and/or Services") provided by PROVIDER to CLIENT pursuant to this document and the agreement entered into between the Provider and the CLIENT (the "Agreement"). PROVIDER must comply with such measures at its own costs, unless it is expressly agreed between the Parties that certain measures herein are irrelevant due to the nature, context and scope of the Goods and/or Services.

1. DEFINITIONS

When the first letter is capitalized, the terms used herein have the meaning set out in the Agreement, unless otherwise specified herein.

Audit Trail(s) means a chronological recording of events, such as creation, modification, deletion and access to record or e-record, that allows reconstruction of the course of events and indicates who created, accessed, changed or deleted data and why.

Client Data means all data, information, text, drawing, picture, video, sound, statistics, analysis and other materials embodied in any form relating to CLIENT or its Affiliated Companies and/or users (where relevant) and/or Goods and/or Services, which may be supplied by CLIENT or its Affiliated Companies (and/or its users) (including Personal Data) and/or to which PROVIDER has access to, generates, collects, processes, stores or transmits and associated Audit Trail in the course of performing the Agreement.

Disaster means any event that causes, or is likely to cause, an adverse effect on the performance of the Agreement including interruption, destruction, quality reduction or other loss of operational capacity of PROVIDER or PROVIDER's Personnel.

Environment means CLIENT's or PROVIDER's current computing and telecommunications environments (consisting of hardware and software) potentially interfaced with the Goods and/or Services that are provided, including the Equipment.

Equipment means all equipment, terminals, infrastructures, related hardware and software, including, as applicable, systems (applications, databases, processing units, personal computers and other processors, controllers, storage devices, printers, phones, other peripherals and input as well as output devices, and other tangible mechanical and electronic equipment intended for the processing, input, output, storage, manipulation and retrieval of data.

IT Change(s) means any actual or proposed change to the nature, level and extent/scope of an Equipment.

Personal Data has the meaning set forth in the Agreement and/or the Data Processing Agreement if applicable.

Professional Standards means, in relation to any particular undertaking or task included, contemplated or envisaged for the performance of the Agreement, those standards, practices, methods and procedures conforming to all Applicable Laws that must be complied with according to the nature of the Services and/or the Goods and/or the Client Data and the presence of Personal Data, and followed with the highest degree of skill, diligence, prudence and foresight that may be reasonably expected of a provider completing similar activities or acting in similar circumstances, and all this in a manner that complies with recognized international standards.

Security Incident has the meaning set forth in the Section 8 "Security Incident Management" of the present document.

Vulnerability means any asset vulnerability or weakness that can be exploited to cause harm to the CLIENT's organization**.** Vulnerabilities can be Critical or non-Critical.

Critical Vulnerability means every Vulnerability with a Common Vulnerability Scoring System (CVSS https://www.first.org/cvss/specification-document) score greater than or equal to nine (9) or Vulnerabilities with a lower CVSS score under specific conditions, including without limitation, if such Vulnerabilities are massively exploited and deemed to represent a significant risk to CLIENT's organization.

Non-Critical Vulnerability means any Vulnerability which is not Critical Vulnerability as defined above.

2. GENERAL SECURITY OBLIGATIONS

Information security contact. PROVIDER shall designate and communicate to CLIENT as single point of contact an IT security responsible individual, (along with a back-up assistant) in charge of the security measures listed herein

Change management. PROVIDER shall implement an IT Change management process to identify changes to the nature, level and extent/scope of any IT system that could impact compliance with any of the obligations set forth herein and immediately report any deviation or breach to the CLIENT.

Information Security and Integrity Program. PROVIDER shall implement and maintain a comprehensive, “Information Security & Integrity Program” applicable to the Goods and/or Services, consistent with Professional Standards, and containing policies and procedures, administrative, technical, and physical safeguards and best practices in order to ensure the security of the Goods and/or Services and Client Data.

Security Assurance Plan. PROVIDER shall implement and maintain a comprehensive security assurance plan describing how PROVIDER will implement, when applicable, each security measure listed in this Appendix. The Security Assurance Plan shall be validated by CLIENT prior to the provision of the Goods and/or Services.

3. ACCESS MANAGEMENT

Access to Client Data. To the extent that PROVIDER has access to Client Data, PROVIDER shall (i) grant access only to authorized PROVIDER personnel with adequate credentials (ii) keep available to CLIENT a regularly reviewed registry of authorized Personnel, (iii) keep access and activities logs and Audit Trails.

Access to CLIENT’s Environment. To the extent that PROVIDER has access to the CLIENT’s Environment, PROVIDER undertakes (i) to comply in particular with CLIENT policies pertaining to the delivery, use and revocation of the identifier(s) and password(s) provided by CLIENT (collectively the "Access Codes"), (ii) to keep all Access Codes provided by CLIENT strictly confidential, (iii) use them only for the purpose of and duration necessary to providing the Goods and/or Services. PROVIDER shall inform immediately CLIENT if it has reasons to believe that such Access Codes have been compromised or are used by third parties. All actions performed through the Access Codes shall be deemed performed by PROVIDER.

Access to CLIENT premises. To the extent PROVIDER is given physical access to Client’s premises (including hosting premises of Client Data), PROVIDER shall (i) ensure that only authorized Personnel is given access (ii) carry out regular physical access rights reviews.

Remote Access. To the extent PROVIDER implements, maintains, or administers any kind of CLIENT’s Equipment remotely, PROVIDER shall (i) comply with CLIENT procedures pertaining to remote access as communicated by CLIENT (ii) keep a record of all action logs during remote access sessions to CLIENT’s Environment and, (iii) only use the remote access means provided by CLIENT.

Monitoring. PROVIDER acknowledges that CLIENT may monitor PROVIDER's activity on CLIENT’s Environment in accordance with Applicable Laws as set out in CLIENT’s Information Technology (IT) and Solutions Usage Policy as communicated by CLIENT.

Passwords Protection. PROVIDER shall ensure that its password policy meets Professional Standards (such as “Password Protection Policy” from SANS Institute or “DAT-NT-001/ANSSI/SDE/NP”).

On-site interventions. To the extent the Goods and/or Services include on-site interventions, PROVIDER shall (i) use CLIENT’s resources only to provide the Goods and/or Services, (ii) comply with CLIENT policies and procedures pertaining to cybersecurity, including on-site Equipment declaration, prior security scans and anti-virus checks, (iii) only use Client Data within CLIENT information system, unless approved by CLIENT, (iv) use only CLIENT-managed Equipment to connect to the Goods and/or Services. In addition, and unless authorized by CLIENT, PROVIDER shall refrain from (i) connecting roaming laptops to CLIENT Equipment and from (ii) using CLIENT's local area network.

4. PERSONNEL

Acceptable Use Policy. PROVIDER shall implement an acceptable use policy (covering teleworking where applicable) that its Personnel shall comply with before accessing PROVIDER's Equipment and/or Client Data.

Ongoing control. PROVIDER shall ensure adequate control over the information security tasks delegated to its Personnel and/or subcontractors on an ongoing basis.

Information security training and awareness program. PROVIDER shall implement and monitor attendance to training programs for its Personnel regarding its security obligations as required by their job responsibilities and all Applicable Laws and Professional Standards

Personnel departure. In case of PROVIDER Personnel departure, PROVIDER shall implement adequate security measures and in particular undertakes that (i) credentials have been deactivated, (ii) CLIENT’s Equipment and Client Data have been returned, (iii) any Client Data stored on a Personnel’s terminal or external media is securely wiped.

5. CLIENT DATA SECURITY

Usage limitation. To the extent PROVIDER hosts, processes, transmits or collects Client Data, PROVIDER shall ensure that PROVIDER will use Client Data exclusively as instructed or authorized by CLIENT under the Agreement.

Secure storage. PROVIDER must ensure the security, confidentiality, availability, and integrity of the Client Data stored on databases, servers, or other forms of non-mobile devices against disclosure, destruction, loss, theft, alteration, access and unauthorized use and access, whether from accidental or malevolent, and all reasonably anticipated forms of compromise, whether by use of state-of-the-art encryption mechanisms, logical access controls, or other robust safeguards.

Datacenter Location. PROVIDER shall communicate to CLIENT all datacenter locations used for the hosting of the Client Data, including those used for backups, prior to the delivery of the Goods and/or performance of the Services.

Encryption. Wherever the Client Data is stored, PROVIDER shall ensure to use encrypted format, in accordance with state-of-the-art cryptography mechanisms. PROVIDER shall ensure that all Client Data is encrypted in transit and at its storage location.

Back-up. PROVIDER shall perform on a regular basis at least once per day two backup copies onto different physical distant locations of (i) Client Data, (ii) associated Audit Trail, and (iii) system configuration. PROVIDER must ensure that back-up is performed in accordance with cybersecurity Professional Standards and in particular that back-up copies (i) are encrypted and protected from crypto-locking attacks, (ii) are stored on reliable media during the duration imposed by Applicable Laws or imposed by CLIENT in the Agreement or any documentation provided to PROVIDER, (iii) maintain the integrity and accuracy of Client Data (iv) can be restored promptly at any time. PROVIDER shall check its ability to restore Client Data at least every 3 years and provide documented evidence to CLIENT in this respect.

6. EQUIPMENT'S SECURITY AND SECURE DEVELOPMENT

Risk assessment plan. To the extent the Goods and/or Services includes an Equipment (hardware or software), PROVIDER shall provide and implement an assessment of the internal and external risks to the security of the Goods and/or Services or Client Data, including identification and evaluation of Vulnerabilities to PROVIDER's Equipment. Such an assessment shall be performed at each major release of its Goods and/or Services.

Cyber Protection and Monitoring. PROVIDER shall ensure at all times that the Goods/Services , any PROVIDER's Equipment are at least secured through antivirus and Endpoint Detection and Response solution (EDR) managed and monitored by a Cyber Security Operation Center. The working hours of the Cyber Security Operation Center shall cover the period during which at least one workstation is connected to the PROVIDER network.

Secure development. To the extent the Goods / Services includes development or integration, PROVIDER shall implement adequate security measures all along the development lifecycle consistent with (i) the OWASP framework (Open Web Application Security Project) and/or (ii) a recognized cybersecurity framework for secure application development and (iii) CLIENT's standards on implementation of the third-party products listed below.

Such measures shall include (i) cybersecurity maintenance contracts with subcontractors, (ii) regular source code review and Vulnerability watch and tests, in particular before move to production (iv) regular patches and updates on software components (included software and container open source packages), (v) segregation of the development environment(s) with the production environment(s), (vi) management of access rights to source code and Client Data, (vii) product and configuration hardening, including deactivation of unused or

outdated functionalities and any type of libraries, change of default credentials including admin passwords, exclusion of uncontrolled source code (viii) control of configuration changes, (ix) exclusive use of only non-production and de-identified data in the development and test environment, unless authorized by CLIENT.

Support and maintenance. PROVIDER shall ensure at all times that the Goods/Services, any component of the solution and/or CLIENT's Equipment (i) are maintained and supported through its subsequent updates and upgrades (ii) have all its component with version no later than N-1, N represents the last up-to-date version of each component (iii) are maintained compatible with all the supported versions of CLIENT components and (iv) are free from any publicly known vulnerability that may impact CLIENT security. PROVIDER shall (i) keep CLIENT informed on It Changes brought to the Goods and/or Services before their release, (ii) notify CLIENT at least a thirty (30) day before any update, (iii) notify CLIENT of the Goods and/or Services end-support/maintenance dates (including all third-party components) at least one year in advance.

Without prejudice to the foregoing, PROVIDER shall (i) implement at all times a security patching process and apply the latest security patches (ii) change passwords for all accounts managed by PROVIDER in accordance with CLIENT's password policy as communicated by Client.

Watch process. PROVIDER shall keep itself informed on threats and Vulnerabilities of the products and technologies implemented on the Equipment it provides or maintains, based on public or private information (including Computer Security Incident Response Team CSIRTs, and Equipment manufacturer's websites).

Vulnerability remediation. In case of discovery of a Vulnerability, PROVIDER shall deploy a remediation solution (i) within a maximum of one (1) month for Non-Critical Vulnerability and (ii) within three (3) calendar days for a Critical Vulnerability . Where not feasible, PROVIDER shall make available to CLIENT within a maximum of three (3) calendar days from Critical Vulnerability discovery a temporary palliative solution at no additional cost and offering equivalent performance and functionality. A definitive solution to the Critical Vulnerability must be provided to CLIENT within a maximum of ten calendar (10) days.

7. INFRASTRUCTURE SECURITY

CLIENT hosting infrastructure. To the extent the Goods and/or Services and/or Client Data are hosted on an infrastructure owned or managed by CLIENT, PROVIDER acknowledges that (i) the Operating System will be a standard CLIENT image with hardened configuration, (ii) CLIENT Equipment is secured through notably antivirus, endpoint detection and response, local password management tool, software distribution agent, filtering and segmentation tools (Firewall, VLAN, etc.) and (iii) compatible systems are integrated into a WINDOWS domain managed by CLIENT.

PROVIDER hosting infrastructure. To the extent the Goods and/or Services and/or Client Data are hosted on an infrastructure owned or managed by the PROVIDER, PROVIDER shall (i) ensure the technical segregation with PROVIDER's other clients' environment and

data (ii) implement and keep available to CLIENT log records to keep track of all actions and/or attempted actions performed on its information system.

8. SECURITY INCIDENT MANAGEMENT

Detection. PROVIDER shall implement adequate procedures and technical measures to detect, track and keep records of all confirmed, attempted or threatened events, whether accidental or malevolent, leading to (i) the unauthorized disclosure, access, use, encryption, reproduction, deletion, loss, theft, alteration, or transmission of Client Data (ii) the unauthorized access (physical or logical), theft or damage to CLIENT's Equipment controlled by PROVIDER, (iii) a disruption of the Goods and/or Services and/or Client Data integrity, functionality or availability, and/or (iv) a breach or potential breach by PROVIDER of its security obligations (collectively "Security Incident").

Notification. PROVIDER shall report to CLIENT within a maximum of twenty-four (24) hours after its discovery, any confirmed Security Incident or any other event that requires notification under Applicable Laws. Such report shall remain confidential and contain all required or useful information to assess the impact and implement mitigation measures.

Remediation and mitigation. PROVIDER should alert CLIENT as soon as any suspected Security Incident that might impact CLIENT. PROVIDER shall mitigate Security Incidents by following an incident management process and adequate response plan (including prevention of future similar events) at its own costs. PROVIDER shall keep CLIENT informed on a regular basis of the progress of its investigation and response plan until the Security Incident has been effectively and totally resolved.

Cooperation. PROVIDER shall fully cooperate with CLIENT in case of any security investigation regarding potential breaches of its obligations.

Disaster recovery and business continuity. To the extent that the supply of Goods and/or Services may be subject to any business continuity breach or Disaster, or unscheduled unavailability, PROVIDER shall ensure the provision of the Goods and/or Services to CLIENT can be resumed, including through alternative measures. PROVIDER shall keep informed and cooperate with CLIENT regarding the unavailability of the Goods and/or Services (including causes, impact, estimated duration).

9. AUDITS AND CONTROLS

Annual Information Security audit. Without prejudice to Client's audit right and remedies as per the Agreement, each calendar year, PROVIDER shall engage at its own costs an independent and nationally recognized audit firm to conduct a security technical configuration audit and penetration tests for internet exposed services. Upon CLIENT's request, PROVIDER shall provide a copy of audit reports and any documentation related to past audits or certifications. In addition, CLIENT shall be entitled to audit PROVIDER, its subcontractors and their systems to monitor compliance with this Appendix.

Vendor assessment platform. PROVIDER shall use CLIENT's standard vendor assessment platform and shall as its own costs (i) aim for a standard score predefined by CLIENT (ii) perform this assessment each calendar year until CLIENT's standards are satisfied and once and if conditions are satisfied (iii) get reassessed every three (3) years.

10. SERVICE LEVEL COMMITMENTS

Security Item	Service Level
Critical Vulnerability CVSS score threshold	9
Critical Vulnerability remediation solution release – Temporary palliative solution	3 days
Critical Vulnerability remediation solution release – Definitive fix	10 days
Non-Critical Vulnerability remediation solution release	1 month
Critical Vulnerability remediation solution deployment	3 days
Non-Critical Vulnerability remediation solution deployment	1 month
Notification of failed antivirus signature update qualification	24 hours
Response delay over a security investigation from CLIENT request	4 hours
Data destruction upon termination of the Agreement	15 days
Equipment return upon termination of the Agreement	30 days
PROVIDER's information system independent security audit frequency	1 year
PROVIDER's response to audit report containing critical findings	15 days
PROVIDER's response to audit report containing no critical finings	20 days
PROVIDER's notice to CLIENT before any IT Changes that impact directly or indirectly the Goods and/or Services	30 days

End of Document