| Exhibit IT Services Provider | | | |
| --- | --- | --- | --- |
| Provider ensures the commitment to satisfy the IT security requirements listed below, in order to guarantee an adequate level of data protection and the compliance with the applicable regulations | | | |
| ID | **Topic** | **Requirement** | **Provider’s answer** |
| 1 | Access control and Authentication | The provider must ensure that:  - an access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing and deleting user accounts - the use of common user accounts is avoided. In cases where this is necessary, it must be ensured that all users of the common account have the same roles and responsibilities - an authentication mechanism is in place, allowing access to the IT system (based on the access control policy and system). As a minimum, a username/password combination must be used. Passwords must respect a certain (configurable) level of complexity - the access control system has the ability to detect and not allow the usage of passwords that don’t respect a certain (configurable) level of complexity - a specific password policy is defined and documented. The policy must include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts - device authentication is used to guarantee that the processing of Generali data is performed only through specific resources in the network |  |
| 2 | Access control and Authentication | The provider implements a user provisioning, deprovisioning, review and change procedures for granting access to systems, data and services, establishing processes and functionalities able to verify the identity of persons (e.g. through ID card, car license, etc.) of each individual user and to promptly remove the access in case of changes (e.g. employees leaving the company). The provider, where possible, shall manage through automated solutions: - an identity management process - an access management process |  |
| 3 | Access control and Authentication | Access rights are assigned following pre-defined authorization steps and their whole lifecycle is governed by a formalized process; only people that strictly need to access to provide the service, according with contract specifications, are authorized to access Generali data. A specific authorization process is established for administrative/privileged and technical users, ensuring an high level of control and traceability. Access rights are promptly removed when no more needed and reviewed ("re-certified") at least every 6 months to ensure that the above-mentioned requirement is continuously enforced). If needed, the Provider supports the review of Generali-managed accounts. If requested by Generali, the provider communicates the list of people accessing applications, systems and data related to Generali (including detail of access rights, date of creation/deletion). |  |
| 4 | Access control and Authentication | The provider implements a two-factor authentication mechanism for remote connections, for accesses with administrative rights, to access all the applications publicly accessible and exposed |  |
| 5 | Business Continuity | The provider must ensure that:  - the organization establishes the main procedures and controls to be followed in order to ensure the required level of continuity and availability of Generali service in case of disruption or unexpected/critical events (including in the event of an incident) - Business Continuity & Contingency Plan and recovery procedures are based on the results of the BIA. They must include clear actions and assignments of roles and they shall be established, documented and validated by the relevant functions - an alternative facility is considered, depending on the organization and the acceptable downtime of the IT systems - the Business Continuity & Contingency Plan is provided to Generali upon request |  |
| 6 | Business Continuity | The provider ensures that the capability of its BCM process and the Business Continuity & Contingency Plan are audited or tested annually. |  |
| 7 | Business Continuity | The provider ensures that its BCM process is compliant with a specific international BCM standard (ISO/IEC 22301:2012 or similarly recognized standard). |  |
| 8 | Data Deletion Disposal | The provider must ensure that: - upon Generali requests and / or in the event of insolvency, resolution or discontinuation of the business operations and / or upon expiration / termination of the contractual relationship, the access, recovery and returning in an easily accessible format of the Generali data and securely, using industry accepted methods and standard formats (e.g. csv) - without prejudice of data return, erase/destroy all or a portion of Generali data in the provider possession are performed according with instructions received by Generali and following the technical requirements described in this document |  |
| 9 | Data deletion Disposal | The provider must ensure that data erasure/destroying will be performed according with the following requirements: - a process is in place to ensure the prompt and secure cancellation of all Generali data, also in case of disposal/reuse of ICT assets - data cancellation must be executed with irreversible methods (multiple overwriting, de-gaussing, physical destruction or equivalent) - in case secure disposal / cancellation is not feasible, the media must be destroyed or rendered unusable, following best practices and standards |  |
| 10 | Data Protection | The provider defines a Data Protection & Classification policy in line with best practices, ensuring the respect of availability, authenticity, integrity and confidentiality principles for the Generali data (including personal data). |  |
| 11 | Data Protection | The provider ensures that operational procedures and documented processes (including roles and responsibilities) regarding the encryption and cryptographic management (e.g. public key infrastructure, cryptographic protocol design and algorithms usage, access controls in place for secure key generation) are formalized and implemented throughout the lifecycle, using cryptographic techniques and practices in accordance with leading practices and standards, with particular reference to the key management (at least revocation, rotation and the key materials secure transmission and storage, including segregation of keys used for encrypted data or sessions). |  |
| 12 | Governance, risk and compliance | The provider communicates the country where it has a registered office and undertakes to provide a list of locations in which the data may be processed (including data processing of subcontractors) and notify, in advance, Generali in case of any change. The provider makes Generali aware of the location of their data and it's not allowed to store data in other location than the one indicated in the contract. In case of subcontracting, the provider shall assess all risks, including security and ICT risks, associated with the location of the potential subcontractors (its parent company and the location where the ICT service is provided from). \*Attach the list or include it inside the Answer and Note field |  |
| 13 | Governance, risk and compliance | The provider that process personal data on behalf of Generali has the following responsibilities: - not to use a sub-processor without the prior written authorization of Generali - to co-operate with supervisory authorities - to ensure the security of its processing - to keep records of processing activities - to notify any personal data breaches to Generali - to employ a data protection officer, if needed - to appoint (in writing) a representative within the European Union, if needed |  |
| 14 | Governance, risk and compliance | The provider must comply with security standards & regulations (ISO27001 and NIST for information security, ISO 22301 for business continuity, or equivalent standards).  The provider shall also perform internal audits at planned intervals to ensure the compliance with the norms. |  |
| 15 | Governance, risk and compliance | All subcontractors involved by the provider, carefully selected, shall respect the requirements included in the contractual agreements defined during acquisition/procurement process and fully comply with the obligations of the service provider. Moreover, the provider shall give assurance that internal organization and data processing arrangements of its sub-processors (if any) are compliant with the applicable local, national and international legal standards of the involved countries. The responsibility of the subcontractors' activities and technologies used to provide the service are in charge of the provider. |  |
| 16 | Governance, risk and compliance | The provider ensures that privileged users with access to Generali data, information systems and supply chain entities involved in the same activities have signed appropriate access agreements (e.g. Non-disclosure or Confidentiality Agreements, Acceptable Use Agreements, Rules of behavior and conflict-of-interest agreements). |  |
| 17 | Governance, risk and compliance | For all projects that are performed through Generali systems and processes, the requirements in this Annex have to be considered in addition to the requirements included in the Generali internal regulations. Each involved entities take visibility of all documents (regulation and annexes) and must comply with. |  |
| 18 | Incident Management | In case of cyber security incident involving the provided service or that could have a direct or indirect impact on Generali, the provider shall: • report to (1) group-cyber-emergency@generali.com for Assicurazioni Generali S.p.A. and to (2) gosp-csirt@generali.com for working hours, +39 041 262 7215 outside of working hours for Generali Operations Service Platform, data breaches and any other cyber security incidents without undue delay and in any case within 4 hours after having become aware of the event. The report shall include at least the following information: - Description of the incident (e.g., systems and services impacted, duration, geographical spread); - Clients impacted (e.g., number of impacted users, amount and/or number of transactions affected); - Consequences of the incident (e.g., service downtime, data losses, data disclosure, system failures); - Remediation (e.g., status of the incident, action taken to mitigate the consequences, further actions suggested) • collaborate with Generali on the incident investigation by providing all the information requested by Generali, in order to guarantee the analysis effectiveness. In particular, the following Provider's contact (e.g. Security Department) and Emergency contact (e.g. Security Operations Center) can be used by Generali: - Provider Contact: [insert email and availability in Provider’s answer]; - Emergency Contact: [insert email and availability in Provider’s answer] • respond to Generali requests of details within 4 hours • provide continuous assistance to Generali at no additional cost • ensure an incident response plan with detailed procedures is defined, periodically reviewed and promptly executed to ensure effective and orderly response to the incident |  |
| 19 | Log Management | The provider implements an automated security information and event management / SIEM tool to facilitate the identification of anomalies and constantly monitor and detect attacks, potential attacks, unauthorized connections and incidents. The tool has to be centralized and has to collect, store, and correlate the various events produced by the systems, devices, applications, and any other information source.  The tool must be able to: - protect the logs from tampering and corruption - correlate data - ensure access control mechanisms and guarantee the need-to-know principle - support industry-standard log collection protocols (e.g., syslog)  The log management platform has to perform correlation between events and allow the creation of automatic notifications and alerts in case of anomalies (including, for example, massive downloads of data).  The monitoring should be performed by a SOC team 7x24. |  |
| 20 | Infrastructure & Network Security | The provider ensures that physical or virtual environments and network connections and data flows are documented (e.g. in terms of diagrams and operational procedures). Such documentation is kept up to date. |  |
| 21 | Infrastructure & Network Security | The provider configures its architecture and infrastructure using adequate security guidelines or standards (DISA, NSA, STIGs, Center for Internet Security, SANS, vendor specific guidelines or other equivalent), maintains proper information systems components with a protection approach (e.g. based on certified Common Criteria) and ensures that applications run in an hardened environment, in compliance with specific operational security requirements, to provide only essential capabilities and prohibits or restricts the use of functions, ports, protocols, and/or services (e.g. FTP, NTP, telnet, RPC, or NFS) that are not necessary to support essential organizational operations. The provider develops, documents and periodically updates a baseline secure configuration of the information system components (including middleware, operating systems, databases, network devices, security devices), according with secure configuration standards. Such baseline is applied to all the new systems and monitored for in-place ones. |  |
| 22 | Infrastructure & Network Security | The provider employs information flow control standards and enforcement mechanisms (e.g. load balancers, gateways, routers, guards, encrypted tunnels, firewalls) to manage information flow between designated sources and destinations (e.g. networks, group of individuals, and devices) within information systems and between interconnected systems. In particular, different network security zones separated by security gateways are established, according to the criticality of systems and information involved (including the segregation between management, monitoring and backup networks) |  |
| 23 | Infrastructure & Network Security | The provider ensures that a virtual firewall scheme is used to isolate tenants / virtual machines / environments. |  |
| 24 | Infrastructure & Network Security | The provider establishes, documents and monitors secure remote access methods to information system (e.g. dial-up, Internet VPN), their usage restrictions (authorization) and configurations (at least encryption). All remote accesses are performed with such secure remote access solution subject to a strong authentication mechanism. |  |
| 25 | Infrastructure & Network Security | The provider ensures that intrusion detection/prevention (IDS / IPS) is handled on the front end, network and virtual machine instances in order to monitor and control the communications at the external boundary of the information system and at the key internal boundaries. Moreover, these tools have to be promptly updated as soon as the signature of new threats is available. |  |
| 26 | Infrastructure & Network Security | The provider's subnetworks for publicly accessible system components are separated from internal networks. |  |
| 27 | Infrastructure & Network Security | The provider shall employ the enforcement of security mechanisms (in particular anti-malware, end-point security system software, EDR or equivalent solutions) to detect and eradicate malicious code (e.g. viruses, worms, Trojan horses and spyware). They are installed, updated and configured on all applicable systems. |  |
| 28 | Infrastructure & Network Security | The provider shall encrypt the Generali data at-rest, in transit and, if applicable, in use.  *\*Specify the protocol used to encrypt Generali data* |  |
| 29 | Infrastructure & Network Security | The provider restricts the access to systems with shared network infrastructure to authorized personnel in accordance with security policies, procedures and standards. |  |
| 30 | Infrastructure & Network Security | The provider identifies and eliminates all single point of failures of critical IT services. Potential exceptions (e.g. due to technical constraints) are documented and related risks are mitigated. |  |
| 31 | Infrastructure & Network Security | Additional security tools (e.g. web application firewalls, XML security gateways for web services, intrusion detection/prevention systems) shall be used and configured to enhance the security of the application while running in operation and to verify and validate the network traffic. Any unauthorized service or traffic has to be blocked. |  |
| 32 | Infrastructure & Network Security | The production environment shall be physically (e.g. different server) or logically (e.g. virtualization) separated from other environments (e.g. development, test, etc.). |  |
| 33 | Infrastructure & Network Security | The provider ensures to, at least every 6 months, review the firewall rule list, according to the classification and overall Risk profile of the system involved, and to ensure that unnecessary or unauthorized rules are removed. |  |
| 34 | Infrastructure & Network Security | The provider ensures that security processes and solutions are implemented to guarantee that connection to all the segments of the internal wired and wireless network is restricted to the authorized devices by Network Access Control (NAC) or equivalent solution, unless organizational or physical protection and access control effectively prevent the connection of unauthorized devices. |  |
| 35 | Physical Security | The provider must ensure that:  - the physical perimeter of the infrastructure is not accessible by non-authorized personnel - clear identification, through appropriate means e.g. ID Badges, for all personnel and visitors accessing the premises of the organization must be established, as appropriate - secure zones are defined and protected by appropriate entry controls. A physical log book or electronic audit trail of all access must be securely maintained and monitored  - intruder detection systems are installed in all security zones - physical barriers, where applicable, are built to prevent unauthorized physical access. - vacant secure areas are physically locked and periodically reviewed  - an automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) is implemented at the server room  - external party support service personnel are granted restricted access to secure areas. |  |
| 36 | Security Assessment | Without prejudice of other audit rights included in this contract, the supplier shall ensure the possibility to perform external security assessments by Generali or by a third party appointed by Generali to verify the implementation of security requirements and the respect of the contractual terms (both in on-site and / or remote assessment mode), sharing required evidences to Generali related to the provider's systems that provide services and / or manage Generali data. The provider shall ensure fully cooperations during the inspection and also allow Generali or the appointed third party to take copies and evidences of the relevant documentation, if necessary. |  |
| 37 | Training | The provider must ensure that:  - the organization has got a regular and structured training programs for provider’s employees on Security topics (e.g. phishing threats, data classification and handling, etc.), including specific programmes for new-joiners  - a training plan with defined goals and objectives must be prepared, executed and reviewed on a regular basis including: 1. a formal information security training program and digital operational resilience training for personnel involved in client access and data management issues 2. a targeted training program for necessary technical skills (e.g. instructor-led training, computer-based training etc.) depending to the context of each job role function. Certifications are recommended - at Generali’s request, provider’s employees will attend Generali’s trainings to raise security and resilience awareness, with a focus on the aspects relevant for the provision of the specific services - the staff has an understanding of Generali data protection threats and concerns relating to the service and to the relevant information risk management policies - all employees are adequately informed about the security controls of the IT system that relates to their everyday work. Employees involved in the processing of Generali data must also be properly informed about relevant data protection requirements and legal obligations |  |
| 38 | VA/PT, Patch Management and Resilience Testing | The provider confirms the availability to participate and fully cooperate in Generali's Threat-Led Penetration Testing (TLPT) in case services provided to Generali are included in the scope of the TLPT. Namely, the provider allows Generali to directly perform tests on the provided services with an external tester or alternatively ensures that it has already entered into contractual arrangements with an external tester, for the purpose of conducting a pooled TLPT on the provided services, under the direction of Generali or another designated financial entity where applicable. |  |
| 39 | VA/PT, Patch Management and Resilience Testing | Periodically and after major releases, the Provider assesses (through vulnerability assessment and/or penetration tests by independent third parties) information systems, infrastructures and applications to ensure that they meet security standards and to identify potential vulnerabilities. Such vulnerabilities are documented, classified (e.g. using simple attack trees or more formal threat modeling process such as Microsoft’s STRIDE, Trike, etc.) and promptly addressed.  In particular, the provider shall execute Vulnerability Assessment at least with a weekly frequency on all the ICT assets. The provider shall execute Penetration Test at least every 1 year for the IT Applications and IT Infrastructure Components. In any case, Penetration Testing on ICT Assets must be performed prior to go-live and, in case of IT major changes, prior to promotion to Production.  The discovered vulnerabilities must be managed in an appropriate way (analysis, determining the root causes, standard classification and remediation, mitigation actions according to criticality, timely performed). In particular: - the scoring of CVSSv3 (or higher version) shall be adopted to determine the severity classification levels - in case of "critical" vulnerabilities (i.e. a score equal to or higher than 9.0) the supplier shall send an immediate communication to Generali including the number of identified vulnerabilities, the impacted systems/data, the severity and the mitigation actions that will be put in place.  Moreover, the provider must provide to Generali, upon request, statistics and trends on vulnerabilities impacting applications and systems related to Generali's service. \*Attach the report of the last VA or PT activity |  |
| 40 | VA/PT, Patch Management and Resilience Testing | External components and third-parties libraries, including open-sources, used by ICT services customised or developed by the provider for Generali shall be: - tracked and evaluated to know if they are needed - identified and checked for known vulnerabilities - monitored in their version and their possible updates - supported by the vendor and updated The tracking and monitoring activities on external components and third-parties libraries, including open-sources, should be performed by the provider also on software off-the-shelf, to the extent possible. |  |
| 41 | Workstation & Mobile security | The provider must ensure that: - users are not able to deactivate or bypass security settings - users not have privileges to install or deactivate unauthorized software applications - the system has session time-outs when the user has not been active for a certain period - critical security updates released by the operating system developer are regularly installed  - anti-virus applications and detection signatures must be configured on a daily basis - transfer critical Generali data from workstations to external storage devices (e.g. USB, DVD, external hard drives) is not allowed - workstations used for the processing of critical Generali data are preferably not connected to the Internet unless security measures are in place to prevent unauthorized processing, copying and transfer of Generali data or store |  |
| 42 | Workstation & Mobile security | The provider must ensure that:  - mobile devices that allow to access the information system must be pre-registered and pre-authorized - mobile devices are subject to the same levels of access control procedures (to the data processing system) as other terminal equipment - specific roles and responsibilities regarding mobile and portable device management are clearly defined - the organization is able to remotely erase Generali data (related to its processing operation) on a mobile device that has been compromised - mobile devices are physically protected against theft when not in use |  |

**Signature of the Supplier’s legal representative**  
  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
  
Position: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
  
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
  
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_