TTEC Supplier Information Security Exhibit

SUPPLIER Information Security Requirements

These requirements constitute minimum information security standards that must be met for the protection and security of TTEC and/or TTEC Client systems, facilities, and data, including Confidential and Personal Information.

Definitions:

Applicable Data Protection Law(s) means any state, federal or foreign law(s), rule(s) or regulation(s) that apply to Supplier's Processing of Personal Data, including those concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling or Processing of Personal Data. For the avoidance of doubt, Applicable Data Protection Law may include, but is not limited to, the following laws when in effect: the European Union General Data Protection Regulation (Regulation (EU) 2016/679) and supplementing data protection law of the European Union Member States (the "**GDPR**"); the United Kingdom Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK Data Protection Laws**"); the ePrivacy Directive (EU Directive 2002/58/EC); the Digital Operational Resilience Act of 2022 ("**DORA**"); the laws, rules, and regulations of each nation in the European Economic Area relating to the protection of Personal Data; the California Consumer Privacy Protection Act of 2018 ("**CCPA**"); the California Privacy Rights Act ("**CPRA**"); Canada's Personal Information Protection and Electronic Documents Act ("**PIPEDA**") S.C. 2000, ch. 5, and any provincial legislation deemed substantially similar to PIPEDA under the procedures set forth therein; the Australian federal Privacy Act 1988 and the Australian Privacy Principles, the Brazilian Lei Geral de Proteção de Datos (Law No. 13,709/2018 – Brazilian General Data Protection Law ("**LGPD**"); the Mexican Federal Law on the Protection of Personal Data held by Private Parties, the Philippines' Data Privacy Act of 2012, Colombian Statutory Law 1266 of 2008 ("**Law 1266**"), the Privacy Act 2020 and Information Privacy Principles of New Zealand, the Swiss Federal Data Protection Act ("**Swiss DPA**"), and the Indian Information Technology Act of 2008.

Applicable Law means any regional, national, and international law, rule, regulation, or standard, including those imposed by any governmental or regulatory authority which apply from time to time to the Party or activity in the circumstances in question. Applicable Laws include Applicable Data Protection Laws.

In-scope Systems means any Supplier or TTEC systems used to access, collect, transmit, process, or store any TTEC and/or TTEC's Client and/or TTEC Client's Customer data.

Information Processing Systems means systems used to process TTEC and/or TTEC's Clients and/or TTEC Client's Customer data.

Confidential Information means information that belongs to TTEC and/or TTEC's Clients and/or TTEC Client's Customer or its affiliates that is critical and sensitive in nature.

Personal Information" means any information that Supplier processes on behalf of TTEC, when such information identifies, is identifiable to, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular Data Subject or the household of a Data Subject.

Personal Identifiable Information (PII) means any data that identifies or can be used to identify an individual.

Sensitive Personal Identifiable Information (sPII) means information that if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII includes, but is not limited to, social security number (SSN), driver's license or state identification number, national identification number (NIN), bank account number, or passport information.

Payment Card Information (PCI) or **Card Holder Data (CHD)** means any identifying data on a credit, debit, prepaid or electronic money card, or any other associated payment card, including the CVV code.

Protected Health Information (PHI) means individually identifiable information that is created or received by a health care provider, health plan, employer, or health care clearinghouse, and is about (i) health status, (ii) the provision of health care, or (iii) the payment for health care that can be linked to a specific individual.

Processing means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, transfer, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

Information Security Incident means (a) any act or omission that compromises or is reasonably likely to have compromised either the security, confidentiality, or integrity of Confidential Information, Personal Information or the physical, technical, administrative, or organizational safeguards put in place by Supplier, or by TTEC should Supplier have access to TTEC's systems, that relate to the protection of the security, confidentiality, or integrity of Confidential Information or Personal Information, or (b) receipt of a complaint in relation to the privacy and data security practices of Supplier or a breach or alleged breach of this Information Security Exhibit relating to such privacy and data security practices. Without limiting the foregoing, a Security Incident shall include any unauthorized use, modification, loss, compromise, destruction, or disclosure of, or access to Confidential Information or Personal Information.

Due Diligence of Supplier's Security, Risk and Compliance Program

Supplier's information security, risk and compliance program is subject to ongoing monitoring and annual reassessment by TTEC. This includes the following:

- Completion of TTEC's Supplier Information Security Risk Assessment at least annually.
- Supplier's information security controls are maintained and reviewed regularly and are designed to meet or exceed current industry, data and technology service compliance standards and regulatory requirements.
- Within ten (10) days of a request being made, an officer of the company will furnish TTEC with a written attestation from a designated representative regarding the company's information security program and a representation and warranty of adherence to its information security program.

Failure to participate in ongoing monitoring and annual reassessment reviews will be considered a material breach under the Master Services Agreement.

Compliance with Privacy and Security Laws

Supplier will remain in compliance with all applicable privacy and security laws and standards, and Supplier's processing CHD/PCI Data will comply with the most current version of the Payment Card Information Data Security Standards (PCI-DSS).

Information Security Program and Responsibilities.

Supplier will develop, implement, and maintain a robust risk-based Information Security Program that is consistent with the requirements of this Exhibit and designed to ensure compliance with the provisions of Applicable Law and Applicable Data Protection Law(s), including as applicable to the Health Information Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Payment Card Industry Data Security Standards (PCI DSS), The Federal Trade Commission Act (FTC Act), Californian Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), The General Data Protection Law (LGPD)) and Sarbanes-Oxley (SOX).

In addition, Supplier's Information Security Program must:

- Protect in scope systems and TTEC's and TTEC's Clients' Confidential and Personal Information, at all times, from internal and external security threats.
- Protect in scope Information from unauthorized disclosure.
- Have controls based on, or mapped to, a recognized information security framework such as ISO/IEC 27002:2013 or National Institute for Standards and Technology (NIST) 800 Series Special Publications.
- Designate one or more privacy and data protection officers who are responsible for overseeing compliance with this Exhibit and provide TTEC with the 24x7 contact information (including email and phone number) for these security representatives.
- Designate a chief information security officer (CISO) (or an equivalent individual) who are responsible for overseeing the information security program and for overseeing the compliance with this Exhibit; provide TTEC with the 24x7 contact information (including email and phone number) for these security representatives.
- Maintain an organization with designated staff adequate to maintain the effectiveness of Supplier's security program and meet TTEC's information security requirements.
- Conduct periodic Risk Assessment of its Information Processing Systems to assess the design and efficacy of its information security program.
- On an annual basis, provide TTEC with a copy of its Information Security Program Policies and Procedures to validate ongoing compliance with a recognized information security framework.
- Promptly notify TTEC of any changes to its Information Security Program that impact services rendered, compliance with industry frameworks, or certification status.

Supplier Security and Privacy Policies.

Supplier Information Security program will implement, maintain, review (at least annually), and enforce a written set of formally adopted and senior management-approved security and privacy policies, procedures, and related documentation which address, at a minimum:

- **Acceptable Use**
- **Access Control**
- **Audit, Logging and Monitoring**

- **Building, Physical and Environmental Security Management**
- **Business Continuity and Disaster Recovery/Crisis Management**
- **Change Management**
- **Clean Desk and Screen**
- **Cloud Computing Management**
- **Compliance Policy Enforcement**
- **Configuration Management**
- **Encryption and Key Management Policy/Requirements**
- **Endpoint Security Management**
- **Ethics Code and Security Awareness Training**
- **Global Privacy Management**
- **Global Technology IT Governance Program**
- **Incident/Security Incident Management and Response Policy/Plan**
- **Information Classification, Labeling, and Handling**
- **Information Security Policy**
- **Information Security Program Commitment/Attestation Statement**
- **Information Security Risk Management**
- **IT Asset Management**
- **Network Security**
- **Password Security Management**
- **Patch Management**
- **Portable Media Security Management**
- **Records, Retention and Destruction Management**
- **Software/System Development Life Cycle Management (SDLC)**
- **Supplier/Vendor Risk Management**
- **Vulnerability Management**

Upon TTEC's request, Supplier will provide any Information Security policy, procedure, or other related documents for review.

Industry Compliance, Audit Reports/Certifications, and Remediation Requirements

At least annually, Supplier will engage a qualified and independent third-party auditing firm to conduct and perform an audit of organizational controls, IT environment, physical and logical controls, safeguards, security policies, and best practices involving the accessing, processing, storing, and transmitting of TTEC and/or TTEC's Clients' Confidential and Personal Information.

The audit will include a review and testing of logical and physical security controls and safeguards, and cover all locations and processes used in support of the business relationship with TTEC.

Remediation of all deficiencies from such inspections, tests, and audits within reasonable timeframes is required.

Upon written request from TTEC, Supplier will provide TTEC with a copy of the final industry compliance audit report, industry compliance certificate and reasonable evidence that any identified deficiencies have been corrected or a specific action plan to remediate those items accompanied by due dates.

In the course of providing Services, if Supplier collects, accesses, processes, transmits or stores any TTEC or TTEC Client financial data, PII, CHD/PCI or Confidential Information, then TTEC requires Supplier to provide, on an annual basis, copies of the applicable audit reports (or its equivalent audit, standard, or assessment reports relating to financial reporting and information protection), issued by a recognized, independent, CPA (Certified Public Accountant), accountancy organization, or authorized third party assessor or certification partner:

A. SOC 1 Type II

B. SOC 2 Type II

C. ISO 27002:2022

D. ISO 27001:2013

E. Payment Card Industry (PCI)

   NOTE (1) Required Documentation: In addition to the PCI Attestation of Compliance (AOC), TTEC also requires submission of a PCI Responsibility Matrix.

   NOTE (2): Any PCI DSS self-assessment/questionnaire is not accepted by TTEC as a qualified/recognized, independent third-party audit assessment. It must be issued by an independent, recognized, PCI Qualified Security Assessor (QSA).

F. FedRAMP (NIST 800-53 Moderate)

G. HITRUST

H. TISAX

I. HIPAA Compliance

If the required qualified, independent, third party attestations of compliance and industry compliance certification(s) are not available, Supplier must obtain such recognized, independent, attestation of compliance and/or industry compliance certification(s), relevant to the Services and in scope systems, within eight (8) to twelve (12) months of the date of the fully executed Agreement and provide to TTEC a copy of required attestation of compliance and/or industry compliance certification(s) for review and approval. TTEC will require status reports from the Supplier throughout the certification/attestation process.

Right to Audit

TTEC maintains the right to audit Supplier (and any Supplier subcontractor) records, systems, and security related to this Exhibit or to the performance of the Agreement upon five (5) business days' prior written notice.

Privacy and Security Awareness Program

Supplier personnel (employees, contractors, subcontractors, service providers and agents provided by temporary staffing companies, if any) must receive comprehensive Privacy and Security Awareness Training within sixty (60) days of hire date (and at least annually thereafter) and prior to gaining access to TTEC or TTEC Clients' Personal and Confidential Information.

Employee Discipline

Supplier must sanction Supplier personnel, including employees, contractors, subcontractors, service providers, and agents, who fail to comply with privacy and information security policies and procedures or any provisions of these Exhibit requirements, including termination of employment/contract relationship where appropriate.

Confidentiality Statement

All persons that will be working with TTEC data, PHI, PCI/CHD, sPII or PII must sign a confidentiality statement that is renewed annually and includes, at a minimum, Information Security Policy, Acceptable Use, Clean Desk and Screen and Ethics Code,

Employee Background Checks.

Background checks are required on all Supplier/Affiliate personnel prior to personnel gaining access to In-Scope Systems and any TTEC Data to the extent permitted by applicable law.

Third Party/Fourth Party Information Security Requirements

Supplier will via a written agreement hold all third and fourth parties, including contractors, engaged by Supplier to the same or substantially similar standards as set forth in this Exhibit.

Access Controls

Supplier will have in place and maintain a formal documented access control policy and procedures that covers ticketing system, approval process, account creation, access provisioning, access reviews, access de-provisioning and account deletion to Supplier's information systems, applications, and sensitive security areas (e.g., Data Centers, MDF rooms, etc.), which contain or process any TTEC and /or TTEC's Client Confidential and Personal Information. This includes access controls that prevent unauthorized access, disclosure, or use of any Confidential and Personal information. All standard user access controls must be assessed and approved for continue access, at least on an annual basis. All administrative and privileged user access accounts must be assessed and obtain management re-approval to continue access, at least quarterly. Upon termination of any Supplier personnel, including contractors and contingent workers provided by staffing agencies, if any, access should be immediately terminated. In no event will access termination occur more than twenty-four (24) hours after employee termination.

Remote Access and Multifactor Authentication (MFA)

A Multifactor Authentication Solution (MFA) (e.g., PingID, Okta, RSA, Cisco DUO, etc.) that adheres to industry-standard requirements is required for all access, including remote access, for all in-scope networks, servers, systems, applications, and software used to support and render services that access, process, transmit or store any TTEC and /or TTEC's Client Confidential and Personal Information.

The MFA solution must provide a new system-generated and system-populated passcode, in addition to the unique user ID and password, before allowing access to in-scope applications and computing devices.

Password Management. Passwords that authenticate users with access to any TTEC and /or TTEC's Client Confidential and Personal Information or Supplier systems that contain any TTEC and /or TTEC's Client Confidential and Personal Information must adhere, at a minimum, to industry standards of PCI DSS Password Requirements and TTEC's Password Security Rules, including User ID and Password Control requirements. Passwords used for in scope systems that are suspected to be compromised must be immediately changed. Passwords will never be displayed or transmitted in clear text. Passwords will be protected using industry standard hashing and salting techniques.

Encryption. Industry standard encryption solution is required for all TTEC and/or TTEC's Client Confidential and Personal Information while data is in transit and at rest on Supplier systems. Encryption solutions will be deployed, with no less than AES 256-bit key for symmetric encryption and a 2048 (or larger) bit key length for asymmetric encryption. For data in transit, Transport Layer Security v1.2 or higher (TLS) with an industry-standard AES-256 cipher, must be supported.

Logical and Physical Segregation. Industry standard physical and logical security controls are required for segregation of all TTEC and/or TTEC's Client Confidential and Personal Information from the data of other Supplier customers.

Data Loss Prevention ("DLP") and Email Monitoring

Supplier will have a Data Loss Prevention program to:

- Continuously monitor, detect and prevent (including notification of senior management) potential data breaches/data ex-filtration transmissions through all endpoints both structured and unstructured TTEC and/or TTEC's Client Confidential and Personal Information while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).
- Actively monitor workforce use of Supplier managed e-mail targeted at data elements typical of TTEC and/or TTEC's Client Confidential and Personal Information.

Any discovery of attempts to send emails containing TTEC and/or TTEC's Client Confidential and Personal Information will be reported to Supplier senior management, and if TTEC and/or TTEC's Client Confidential and Personal Information has left Supplier's control, it will be treated as an Information Security Incident requiring Supplier to notify TTEC.

Non-Supplier managed e-mail or communication solutions will not be permitted to be used to conduct Supplier business related to TTEC without the express written consent of TTEC as part of a clear business requirement.

IT Asset and Information Management. Supplier will maintain an inventory of all TTEC's and /or TTEC's Client Confidential and Personal Information in its possession and the physical assets used to access, transmit, store and process that information, and will include application and database controls to prevent integrity routines, including, but not limited to, processing errors, corruption of data and/or misuse. Supplier will categorize and handle TTEC's data by complying to a recognized industry standard compliance framework (e.g. PCI, SOC 2 Type II, ISO 27001/2, etc.)

Upon termination of any Supplier Personnel, including contractors and contingent workers provided by staffing agencies, if any, Supplier must obtain all Supplier equipment (e.g. laptops, PCs, tablets, mobile devices, etc.), ID badges and any other access badges on the day of termination to limit the risk of an individual acting out, rogue or negative behavior, to obtaining or exposing any TTEC's and /or TTEC's Client Confidential and Personal Information. All equipment used to support the Services must be scanned and declared "clean" of any wrongdoing or unauthorized access or exposing of any TTEC's and /or TTEC's Client Confidential and Personal Information.

Personal Devices. Supplier will ensure Supplier Personnel, including contractors and contingent workers provided by staffing agencies, if any, will not be permitted to, and will not, utilize personal computing equipment (e.g., PCs, mobile devices, cell phones, tablets, etc.) for accessing, processing, storing, or transmitting any TTEC's and /or TTEC's Client Confidential and Personal Information.

Removable Media. Except in the context of Supplier routine back-ups or as otherwise specifically authorized by TTEC in writing, Supplier will institute strict physical and logical security controls, all removable media must be in encrypted format (AES 256), aligning to industry standards, to prevent transfer of any TTEC's and /or TTEC's Client Confidential and Personal Information to any form of Removable Media. In general, removable media is not permitted. Any use of removal media must have a completed exception approved by the TTEC CISO.

Transportation of Physical Media. Supplier will transfer all TTEC and /or TTEC's Client Confidential and Personal Information in physical form in secure containers or packaging.

Destruction of Physical Media. Destruction of physical media, such as printed documents, containing any TTEC and /or TTEC's Client Confidential and Personal Information will be performed in accordance with NIST 800-88 guidelines.

PAPER DOCUMENT CONTROLS AND/OR EXPRESS WRITTEN CONSENT FROM TTEC (IN ACCORDANCE WITH TTEC **REMOVABLE MEDIA** REQUIREMENTS, WHERE APPLICABLE) APPLY TO THE FOLLOWING:

- **A.** ***Supervision of Data***
- **B.** ***Escorting Visitors***
- **C.** ***Confidential Destruction***
- **D.** ***Removal of Data***
- **E.** ***Faxing***
- **F.** ***Mailing***

Physical and Environmental Security. Supplier will employ physical entry controls to restrict access to areas where TTEC and /or TTEC's Client Confidential and Personal Information is accessed, collected, stored or processed solely to SUPPLIER's personnel authorized for such access. Supplier must follow industry standard practices, such as "ASHRAE TC 9.9", for infrastructure systems, including fire extinguishing, cooling, power, emergency systems and personnel safety in mission critical facilities such as data centers.

Telecommunication and Network Security. Supplier will implement and maintain a secure network architecture combining, industry standard, hardening and configuration security controls and safeguards with operating best practices and complying to operational security policies.

Firewalls. Supplier will maintain current layer 7, content filter firewall technology in the operation of SUPPLIER'S environments. Traffic between TTEC and Supplier will be protected and authenticated by industry-standards, and TTEC approved cryptographic technologies.

Firewall Maintenance. At a minimum, Supplier will review firewall rule sets, at least quarterly, to ensure that legacy rules are removed, and active rules are configured correctly.

Intrusion Detection and Prevention. Supplier will deploy intrusion detection and prevention systems (NIDS/NIPS) to monitor the network for inappropriate activity.

EndPoint Detection and Response Solution (EDR). Supplier will deploy and maintain an EndPoint Detection and Response Solution (EDR), on all endpoints that access, collect, process, transmit or store TTEC and /or TTEC's Client Confidential and Personal Information, to protect against viruses and malware. The platform solution must use a combination of machine learning, behavioral analytics, and artificial intelligence, in addition to using malware signature, to consistently protect critical in-scope endpoints and to ensure that systems are not exposed to any mode of cyber-attack.

Log Management. Supplier will deploy a log management solution and retain logs produced by all relevant network devices and IT systems including, but not limited to, firewalls and intrusion detection systems for a minimum period of eighteen (18) months, and logs will only be accessible to only those authorized employees that have a business need to review or access them. All logs must be stored using an industry standard encryption solution (AES 256).

Wireless Security. If Supplier deploys a wireless network, Supplier will maintain written policies governing the use, configuration, and management of wireless networks. All wireless networks deployed must include industry standards and best practices. All wireless network devices will be protected using appropriate physical controls to minimize the risk of theft, unauthorized use, or damage.

Rogue Access Point Detection. Supplier will maintain a program to detect rogue access points at least quarterly to ensure that only authorized wireless access points are in place.

IoT Detection and Assessment. Supplier will maintain a program to detect and evaluate Internet of Things (IoT) devices (e.g., Smart HVAC) at least quarterly to ensure that such devices do not impose any risk to the security of systems which store or process TTEC and /or TTEC's Client Confidential and Personal Information and are managed in accordance with Supplier's security program.

Device Hardening. Supplier will implement and maintain industry best practices and standards of hardening Supplier systems (including servers, endpoints and other devices) to make them less vulnerable to security issues, vulnerabilities and security threats (e.g., NIST 800-53, PCI-DSS, HITRUST).

Vulnerability Management. Supplier must run internal and external network vulnerability scans, including Port Scans, at least quarterly, and after any material change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades). At least annually, Supplier will provide to TTEC, an executive vulnerability scan and test summary report of all relevant systems used to render services.

Penetration Management. Supplier must perform internal penetration testing, at least quarterly, and after any material change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades). Supplier will provide, at least once annually, an executive summary of the penetration testing report and executive summary of test results (performed at least annually by a qualified, independent Penetration Auditing Firm) showing all vulnerabilities have been remediated.

Patch Management. Supplier will patch all systems and endpoints, such as workstations, and servers with all current operating system, database and application patches deployed in Supplier's computing environment according to a schedule predicated on the criticality of the patch.

Licenses and Software Development:

Software Usage. Supplier will not attempt to copy, alter, decompile, reverse engineer, or disassemble any of the software programs contained in TTEC Information Systems.

Software Development. If the Services include the development of software product(s), including web applications, for TTEC, such software will be developed and maintained in accordance with industry standard development methodology.

Systems Development Life Cycle (or "SDLC"). Supplier will maintain a Systems Development Life Cycle (or "**SDLC**") program and process in line with industry standards and best practices.

Threat Modeling. Supplier must use an industry accepted threat model methodology to identify emerging cyber risks and risk scenarios which pose a threat to any and all Supplier systems, applications and third parties which store, transmit or process any TTEC and /or TTEC's Client Confidential and Personal Information or impact the services contracted to TTEC.

Software Documentation and Application Development Training. Supplier will maintain documentation on overall system, network and application architecture, data flows, process flows, and security functionality for all applications.

Change Management. Supplier will employ an effective, documented change management program, such as ITIL, with respect to the Services as an integral part of its security profile. Changes that could impact the services being delivered to TTEC must obtain a written consent from TTEC before changes are implemented.

Cloud/Virtual Environments. Supplier, to the extent that it uses computing technology that is virtual in nature, will implement appropriate controls and monitoring systems.

Information Security Incident Management. Supplier will establish, test, and maintain an information security incident response program that adheres to a recognized industry standard (PCI, ISO 27001/2). Supplier will notify TTEC in the event of any Information Security Incident within 24 hours of identification. Interim and detailed reports regarding the incident will be provided to TTEC within 72 hours.

Business Continuity and Disaster Recovery/Crisis Management. Supplier will establish and maintain a Business Continuity and Disaster Recovery (BCDR) Resiliency Management program that should meet or exceed ISO 22301standards.

Access to TTEC Premises/Facilities. Compliance with guidance, policies and requirements provided by TTEC is required for the entire duration of the engagement if Supplier is provided physical access to TTEC Premises.