# Security Measures Attachment

2026-01-28 - India

This Security Measures Attachment sets forth the security controls and requirements applicable to the Cloud Services. This document constitutes an Attachment to the Agreement. Capitalized terms not defined herein shall have the meanings given in the SaaS GTC.

The technical and organizational measures described in this Attachment are designed to protect the confidentiality, integrity, and availability of the Cloud Services and Client Data, and are based on international standards and generally accepted industry practices.

Optel may update or modify the technical and organizational measures herein from time to time, provided that such modifications do not materially decrease the overall level of security of the Cloud Services and Client Data.

| Domain | Practices |
|---|---|
| **Organization of Information Security** | **Security Responsibility:** Optel has appointed one or more security officers responsible for coordinating and monitoring security rules and procedures.<br>**Security Roles and Responsibilities:** Optel personnel with access to the Client Data are subject to a confidentiality obligation through their employment contract.<br>**Risk Management Program:** Optel conducts periodic risk assessments on these services or when significant changes are made.<br>**Optel retains its security documents** pursuant to its retention requirements after they are no longer in effect. |
| **Asset Management** | **Asset Inventory:** Optel maintains an inventory of all media on which Client Data is stored. Access to these inventories is restricted to Optelpersonnel authorized in writing to have such access.<br>**Asset handling:** Optel classifies Client Data to help identify it and to allow for access to it to be appropriately restricted.<br>**Optel imposes restrictions on the printing** of Client Data and has procedures for disposing of printed materials that contain such data.<br>**Optel personnel must obtain Optel's authorization** prior |

| | |
|---|---|
| | to storing Client Data on portable devices, accessing this data remotely or processing this data outside Optel's facilities. |
| **Human Resources Security** | **Safety Training:** Optel informs its personnel about relevant security procedures and their respective roles. Optel also informs its personnel of possible consequences of breaching the security rules and procedures. Optel only uses anonymous data in the training of its personnel. |
| **Physical and environmental security** | **Physical Access to facilities:** Optel limits access to facilities where information systems that process Client Data are located to identified authorized individuals.<br>**Physical Access to Media:** Optel maintains records of the incoming and outgoing media containing Client Data, including the kind of media, the authorized sender/recipients, the date and time, the number of media and the types of such data they contain.<br>**Protection from disruptions:** Optel uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.<br>**Media Disposal:** Optel deletes Client Data using procedures that comply with industry standards. |
| **Communications and Operations Management** | **Operational Policy or Procedures:** Optel maintains security documents describing the applicable security measures and procedures, as well as the responsibilities of its personnel having access to Client Data.<br>**Data Recovery Procedures:**<br>● On a regular basis, but in no case less than once a week (unless no update has occurred during this period), Optel maintains multiple copies of Client Data from which such data can be recovered.<br>● Optel stores copies of Client Data and data recovery procedures in a different place from where the primary computer equipment processing the Client Data.<br>● Optel has specific procedures in place governing access to copies of Client Data.<br>● Optel reviews data recovery procedures annually, except for data recovery procedures for Professional Services.<br>**Malware:** Optel has implemented anti-malware measures to protect Client Data against unauthorized access attempts, including malicious software originating from public networks. |

| | |
|---|---|
| | **Data beyond Boundaries:**<br>● Optel encrypts or enables Client to encrypt Client Data that is transmitted over public networks.<br>● Optel restricts access to Client Data stored on media leaving its facilities.<br>**Event Logging:** Optel logs, or enables Client to log, access and use information systems, containing Client Data, register the access ID, authorization granted or denied, and relevant activity. |
| **Access control** | **Access Management Policy:** Optel maintains a record of security privileges of individuals having access to Client Data.<br>**Access Authorization**<br>● Optel maintains and updates a record of personnel authorized to access Client Data.<br>● Optel deactivates authentication credentials that have not been used for at least six (6) months.<br>● Optel identifies those personnel who may grant, alter or cancel authorized access data and resources.<br>● Optel ensures that where more than one individual has access to systems containing Client Data, the individuals have separated identifiers/log-ins.<br>**Least Privilege**<br>● Technical support personnel are only permitted to have access to Client Data when needed.<br>● Optel restricts access to Client Data to only those individuals who require such access to perform their job function.<br>**Integrity and Confidentiality**<br>● Optel instructs Optel personnel to disable administrative sessions when leaving premises Optel controls or when computers are otherwise left unattended.<br>● Optel stores passwords in a way that makes them unintelligible while they are in force.<br>**Authentication**<br>● Optel applies procedures that comply with industry standards to identify and authenticate users attempting to access its information systems.<br>● For password-based authentication mechanisms, Optel requires that passwords be renewed regularly.<br>● For password-based authentication mechanisms, Optel requires that passwords contain at least eight |

| | |
|---|---|
| | (8) characters.<br>● Optel ensures that deactivated or expired identifiers are not granted to other individuals.<br>● Optel monitors, or allows the Client to monitor, repeated attempts to gain access to the information systems using an invalid password.<br>● Optel uses industry-standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.<br>● Optel uses industry-standard password protection procedures, including to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.<br>**Network Design:** Optel has implemented controls to prevent individuals from accessing Client Data using unauthorized access rights. |
| **Information Security Incident Management** | Incident response process:<br>● Optel maintains a record of security breaches with a description of the breaches, the time period, the consequences of the breaches, the name of the reporter and to whom the breach was reported, and the procedure for recovering data.<br>● For each security breach, a notification will be sent by Optel without undue delay and, in any event, within seventy-two (72) hours.<br>● Optel tracks, or allows the Client to track, disclosures of Client Data, including what data has been disclosed, to whom, and at what time.<br>**Monitoring of Services:** Optel reviews logs on a regular basis in accordance with its internal security policies. |
| **Business Continuity Management** | **Optel maintains emergency and contingency plans** for the facilities in which Optel information systems process Client Data in accordance with the relevant Documentation.<br>**Optel's redundant storage systems and data recovery procedures** are designed to attempt to reconstruct Client Data to the original state or last-replicated state from before the time it was lost or destroyed. |