# Technical and Organizational Measures

| | |
|---|---|
| **Measures of encryption of personal data** | TierPoint encrypts laptops and workstations that could access personal data and requires the use of secure ports and protocols (SSH, HTTPS, RDP, etc.) using TLS 1.2 or above when transmitting sensitive information.<br>Encryption of data within customer environments and in-transit may be implemented by the customer or via additional services from TierPoint.<br>Customers are responsible for the pseudonymisation of personal data prior to transferring it to TierPoint |
| **Measures for ensuring ongoing confidentiality, availability and resilience of processing systems and services** | TierPoint enhances the confidentiality, availability and resilience of processing systems that service customers through the implementation of redundant and secure infrastructure that undergoes regular security scanning and availability testing.<br>Customers may purchase high availability environments from TierPoint or implement their own redundant processing systems. |
| **Measure to quickly identify and manage security and availability incidents to resolution** | TierPoint maintains formal incident management procedures for the handling of security and availability incidents including initial detection/reporting, classification, handling, escalation/communication activities, service restoration and root cause analysis. |
| **Measures for ensuring the ability to restore the availability and access to personal Data in a timely manner in the event of a physical or technical incident** | TierPoint has implemented business continuity, disaster recovery and restoration processes to meets its own recovery point and time objectives and as well as the service level objectives of services managed from that TierPoint infrastructure.<br>TierPoint has also implemented DDoS mitigation infrastructure to protect TierPoint and its customers from DDoS attacks. Customers are protected from two attacks but must purchase addon DDoS mitigation services to be protected from future attacks.<br>Customers may purchase additional backup and disaster recovery and restoration services from TierPoint to protect personal Data or implement their own solutions. |
| **Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing** | TierPoint is ISO 27001 certified and undergoes annual 3rd party audits against SOC 1, SOC 2, NIST SP 800-53 and others. TierPoint also conducts annual and quarterly internal audits and assessments throughout the year to ensure that security measures are operating effectively. |

| | |
|---|---|
| **Measures for user identification and authorization** | TierPoint requires its personnel to use a unique user id and password to authenticate and access internal TierPoint infrastructure systems which are used to manage customer environments. TierPoint personnel are prohibited from logging into any TierPoint system or network anonymously and from sharing account credentials. System privileges require role-based and least access principles and are revoked upon termination of employment. |
| **Measures for the protection of Data during transmission** | Remote access to TierPoint's internal networks and systems is restricted via VPN tunnel and end-to-end encryption requiring a unique user id, password and multi-factor authentication.<br>TierPoint requires the use of HTTPS encryption for data in transit (using TLS 1.2 or above).<br>Encryption of data in-transit may be implemented by the customer or via additional services from TierPoint. |
| **Measures for the protection of Data during storage** | TierPoint has deployed a variety of disk, application and file encryption technologies to protect data at-rest and offers add-on encryption services to customers to meet their data protection needs.<br>Encryption of data within customer environments may be implemented by the customer or via additional services from TierPoint. |
| **Measures for ensuring physical security of locations at which personal Data are processed** | TierPoint has implemented the following physical security control at its data centers:<br>Physical access protection (e.g., steel doors, windowless rooms or secured windows)<br>Two-factor electronic access control system to protect secure areas<br>Monitoring of the facility by security services and access logging to the facility<br>Role-based access to infrastructure systems and sensitive power, cooling and electrical infrastructure reviewed at least quarterly<br>Video surveillance (retained for at least 90 days) of all security-relevant security areas, such as entrances, emergency exits to data centers and server rooms<br>Central assignment and revocation of access control authorization<br>Identification of all visitors by verification of their identity card and registration (a log of visitors is kept for at least one year)<br>Mandatory identification within the security areas for all TierPoint personnel, vendors and visitors<br>Visitors must be always accompanied by personnel |

| | |
|---|---|
| | Customers may purchase additional physical security services such as badge readers for cabinet and/or cages from TierPoint and may implement fixed cameras within their own cabinets and/or cages. |
| **Measures for ensuring events logging** | TierPoint has implemented centralized security and availability log monitoring of its infrastructure.<br>Customers may purchase add-on log retention and review services from TierPoint or implement their logging management solution. |
| **Measures for ensuring system configuration, including default configuration** | TierPoint's Configuration Management Policy requires the creation and maintenance of asset inventories and configuration management plans for TierPoint infrastructure systems. |
| **Measures for patch and vulnerability management** | TierPoint Patch and Vulnerability Management Policy requires the use of anti-virus, malware detection, management of vulnerabilities by implementing security patches, hot fixes and firmware updates. TierPoint patching is prioritized by criticality. |
| **Measures for internal IT and IT security governance and management** | TierPoint has implemented governance and management oversight of its Information Security Management System (the 'ISMS') that meets AICPA SOC 2 COSO requirements and is ISO 27001 certified.<br>TierPoint requires all TierPoint personnel to complete security and privacy awareness training at initial hire and annually thereafter with additional technical training required for personnel supporting TierPoint and TierPoint customer systems. |
| **Measures to provide oversight and control of approved documents** | TierPoint has implemented a formal Document Control Management process to provide oversight, approval and control of approved policies, procedures and standards using standard templates, a centralized repository and communication of new and updated documents. |
| **Measures for certification/assurance of Processes and products** | TierPoint is ISO 27001 certified and undergoes annual 3rd party audits against SOC 1, SOC 2, NIST SP 800-53 and others. |
| **Measures for ensuring Data minimization** | TierPoint collects limited personal data types for its own documented business purposes. |
| **Measures for ensuring Data quality** | TierPoint manages the quality of data that it collects for its own use by providing customers the ability to self-manage their authorized contact lists in the TierPoint Support Portal.<br>Customers are responsible for maintenance of their own authorized contact lists and the timely update or removal of any personal data with TierPoint's Support Portal. |
| **Measures for ensuring limited data retention** | TierPoint limits the length it retains data according to TierPoint's documented business purposes and applicable legal, regulatory, and contractual retention requirements. |

| | |
|---|---|
| | Customers are responsible for defining and implementing their own data retention processes and solutions. |
| **Measures for ensuring accountability** | TierPoint conducts background checks and multi-panel drug screens on all employee at time of hire.<br>TierPoint requires all employees to review and sign the Employee Handbook that contains covers TierPoint's philosophy, culture, codes of conduct, ethics, acceptable use policies and other personnel topics.<br>TierPoint also provides employees with 3rd party ethics reporting tool where employees can anonymously report violations of the law, safety, security, ethics and other prohibited activities.<br>TierPoint requires all personnel to sign confidentiality agreements at initial hire. TierPoint also performs data protection impact assessments to assess TierPoint's handling of personal data it gathers.<br>TierPoint has implemented a Sanctions Policy to provide guidance and consistency in the enforcement of security and privacy policies using a progressive disciplinary process up to and including termination of employment. |
| **Measures for allowing Data portability and ensuring erasure** | TierPoint services allow customers to copy their data another services provider prior to termination. TierPoint has also implemented media deletion and destruction policies for various types of media that contain customer personal data.<br>Customers are responsible for determining the level of data sanitization required for their personal data and implementing or purchasing the services appropriate for those requirements.<br>TierPoint offers various additional media destruction or retention services for dedicated hardware. |