

Telappliant Security Statement

Telappliant takes its business security and privacy concerns seriously. We utilise industry standard security measures to ensure customer and user data is kept secure, safe and only accessible to those authorised. This Security Statement details our security measures and practices for our customers and users.

Physical Security

Telappliant servers are located in a SAS70 Type II certified data centre with:

- Four redundant power systems from separate grids with N+1 standby generators for 100% availability
- High power air conditioning units in an N+2 configuration and provides full function, closed control air conditioning with cooling, humidity and de-humidification control
- Secure and monitored single-person point of entry, with integrated digital video camera surveillance, physically guarded 24/7

Network Security

- Firewall restricts access to all ports except http and https
- Intrusion detection systems and other systems detect and prevent interference or access from outside intruders
- Daily scan using Sophos Endpoint Security and Control
- Security-related events are monitored 24/7 by Telappliant's first line support team. Logs and audits show events such as port-scan attacks and unauthorised access to accounts. Anomalous occurrences are investigated and corrective measures taken immediately

Data Security

- Telappliant employees do not have access to customer data, except where necessary for system management, maintenance, monitoring, backups and support
 - Data is stored using RAID disks and storage clusters
 - Database connections are limited to only authorised internal networks, via encrypted VPN
 - Telappliant secures all personally identifiable information on servers in a controlled, secure environment, protected from unauthorised access, use or disclosure
 - Personal information (such as credit card number) transmission is protected through the use of encryption, including the Secure Socket Layer (SSL) protocol
-

User Security

- Employee access into the workplace is through biometric scanning. All clocking in and clocking out is mandatory and monitored
- Proximity card access is provided from the main data centre building and is issued to provide access only to authorised facilities management suites
- Deep penetration testing and audits are performed by authorised external vendors
- Telappliant is audited quarterly by PCI DSS approved scanning vendors
- Telappliant does not sell, rent or lease its customer lists to third parties
- Telappliant does not use or disclose sensitive personal information without the explicit consent of the customer or user
- Telappliant keeps track of our websites and pages that customers visit. This data is used to deliver content and advertising within our websites and pages to customers interested in specific products and services
- Telappliant websites will disclose your personal information without notice, only if required to do so by law or in the good faith belief that such action is necessary to (a) conform to the edicts of the law or comply with legal process served on Telappliant or the site; (b) protect and defend the rights or property of Telappliant; or (c) act under exigent circumstances to protect the personal safety of Telappliant customers or users, or the general public

Business Continuity

- Data centre fire detection and suppression procedures are in compliance with BS 5839, 6266, 5445, 5306, 3115 and 5588, ensuring that any possible customer disruption is minimised and that any minor problems remain localised
- Telappliant policies and procedures for emergency and disaster recovery are developed and implemented to maintain or restore operations and ensure availability of information and data at the required level and in the required timescales
- Telappliant policies and procedures for emergency and disaster recovery are tested and updated regularly to ensure they are up to date and effective
- Telappliant is committed to providing services to customers and conducting business in an ethically and socially responsible manner that respects the environment

Enforcement

Telappliant takes the security of its business, customers and users very seriously. If any employee is found to have breached the Company's code of conduct and its policies and guidelines on security, the employee is immediately disciplined and if applicable prosecuted according to law.