ORBCOMM - Technical and Organisational Measures

1. Security Measures

1.1. ORBCOMM will use appropriate technical and organizations measures to protect Customer data as required by applicable privacy laws and in accordance with industry standard security practices. The following is a list of technical and organizational measures implemented by ORBCOMM.

1.1.1. Governance, Risk Management and Compliance

1.1.1.1. Information Security Program

ORBCOMM has established an enterprise-wide information security program aimed at safeguarding the confidentiality, integrity and availability of all information assets and ensure regulatory, operational and contractual requirements are fulfilled.

1.1.1.2. Right to Audit and Audit Finding Remediations

Third-party audit requirements are negotiated and executed per contract terms and conditions. Audit findings are remediated by raising an issue. Each issue is tracked through a change management process with a defined remediation plan and ownership assigned.

1.1.1.3. Threat Intelligence

Threat intelligence gathering is in place with constant evaluations of our adversaries to determine the most effective controls.

1.1.1.4. Risk Management

Risk assessments are conducted by multiple functions in ORBCOMM. Each function identifies different sources of risk to ORBCOMM and prioritizes mitigation based on several factors including, but not limited to severity, affected products and/or services, and timeline for remediation. Risk mitigation plans are recorded and implemented through the risk management process. All risks are assigned mitigation plans, which are tracked with the risk owner.

1.1.2. Access Control

1.1.2.1. Authorization

ORBCOMM enforces authorization controls for remote and wireless access to the company network prior to allowing such connection. System access and privileges are limited based on the types of transactions and functions authorized users are permitted to execute.

1.1.2.2. Least Privileges

ORBCOMM limits access to those who have a specific need to access systems and data. User access is only approved for the minimal requirements or least privilege necessary for an individual to perform job responsibilities.

1.1.2.3. Account Management

ORBCOMM manages identification, authentication, and access rights for all users. Reviews of active users are conducted periodically to ensure only authorized individuals have access to information systems. EntraID access is contingent upon employment status, when there is a change in status in the HR system, access is automatically revoked.

1.1.3. Network Security

1.1.3.1. Defense in Depth Architecture

Defense in depth strategy is employed, including network hardening and patching, log collection and correlation, and deny all/permit by exception firewall configuration.

1.1.3.2. Boundary Protection

Boundary protection is through managed firewalls. Network perimeter security is maintained through endpoint protection, intrusion detection and prevention systems and firewalls.

1.1.4. Physical and Environmental Security

1.1.4.1. Physical Security Protections

Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) are implemented to safeguard sensitive information and information systems.

1.1.4.2. Limit Physical Access

Physical access to facilities and data centers is restricted in order to protect hosted information, applications, systems, and infrastructure. Controlled access points limit physical access to IT assets. All external access points require approved security controls. Access to the site is controlled by an approved mechanical and electronic access control system.

1.1.4.3. Visitor Access Control

All visitors must provide a government issued ID to enter the facility and be issued and wear a temporary access badge. Identification badges are used, and visitors must be accompanied by an escort. Visitor access is subject to approval and is maintained in accordance with ORBCOMM retention policy.

1.1.5. Product Security

For more information on ORBCOMM's Product Security Policy, please visit Product Security Policy | ORBCOMM.

1.1.6. Personnel Security and Training

1.1.6.1. Onboarding New Hires

Hiring procedures for new employees require the completion of a detailed application form as allowed by local law and appropriate for job roles, including educational verification, previous employment verification, Social Security Number (SSN), National Identifier or Personal Identity Code validation, drug screen and criminal history check.

1.1.6.2. Awareness and Training

Annual compliance training for employees to complete an online course and pass an assessment covering information security and data privacy. The security awareness program may also provide materials specific to certain job functions.

1.1.6.3. Personnel Termination

Terminations are initiated by the employee's supervisor. Cyber access is contingent upon employment status. Access revocation is immediately and automatically triggered by changes to status of employees or contractors in the HR system.

1.2. Customer is solely responsible for determining whether the security controls outlined in Appendix 1 Section 1 of this agreement meet its requirements and provides a level of security appropriate to the risks of processing such customer data. Customer acknowledges and agrees that the level of security outlined in Appendix 1 Section 1 is appropriate to the risk inherent in the processing of data by ORBCOMM on behalf of the customer. Customer is responsible for configuring the services in a manner which enables Customer to comply with applicable privacy laws, including the implementation of appropriate technical and organizational measures.

2. Access And Confidentiality

ORBCOMM will ensure that only authorised personnel who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality may access Customer Personal Data for the purposes of performing the services under this Agreement.

3. Prohibited Data

Customer acknowledges and agrees that ORBCOMM prohibits the submission of certain types of Personal Data (such as a PCI or health information) to the services. Customer will not submit to the services any Customer Personal Data which is regulated by COPPA, FERPA and HIPAA unless authorised to do so in writing by ORBCOMM.