TECHNICAL AND ORGANIZATIONAL DATA SECURITY MEASURES

Contents:

Introduction

This Technical and Organizational Data Security Measures articulates the technical and organizational security measures implemented by FreeConferencing Corp ("CARRIERX") in support of its Information Security Program.

Definitions

"CARRIERX" means FreeConferencing Corp, and all of its direct and indirect subsidiaries.

"Customer" means any purchaser of any CARRIERX offering.

"Personal Data" means any information directly or indirectly relating to any identified or identifiable natural person.

"Sensitive Personal Data" means Personal Data (1) consisting of an individual's first name and last name, or first initial and last name, in combination with some other data element that could lead to identify theft or financial fraud, such as a government issued identification number, financial account number, payment card number, date of birth, mother's maiden name, biometric data, electronic signature, health information, or (2) consisting of log-in credentials, such as a username and password or answer to security question, that would permit access to an online account or an information system; or (3) revealing the personal health information (PHI) of a natural person.

"Information Security Program" refers to the collection of CARRIERX's policies and procedures governing information security, including, but not limited to, policies, trainings, education, monitoring, investigation and enforcement of its data management and security efforts.

The Technical and Organizational Data Security Measures

CARRIERX has implemented and maintains a security program that leverages the PCIDSS and ISO/IEC 27000-series of control standards as its baseline.

Access Control of Processing Areas

Web applications, communications infrastructure, and database servers of CARRIERX are located in Tier2 secure data centers in United States. CARRIERX has implemented suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where Personal Data are processed or used.

This is accomplished by:

- Establishing security areas;
- Protection and restriction of access paths;
- Securing the data processing equipment and personal computers;
- Systems developed to provide Data-at-Rest protection with industry standards encryption mechanisms
- Establishing access authorizations for employees and third parties, including the respective documentation;
- Restricting physical access to the servers by using electronically-locked doors and separate cages within co-location facilities;

- Access to the data center where Personal Data are hosted is logged, monitored, and tracked via electronic and CCTV video surveillance by security personnel; and
- Data centers, where Personal Data may be hosted, are protected by security alarm systems, and other appropriate security measures, such as user-related authentication procedures, including biometric authentication procedures (e. g., hand geometry), and/or electronic proximity identity cards with users' photographs.

Access Control to Data Processing Systems

CARRIERX has implemented suitable measures to prevent its data processing systems from being used by unauthorized persons.

This is accomplished by:

- Establishing the identification of the terminal and/or the terminal user to the CARRIERX systems;
- Automatic time-out of user terminal if left idle, identification and password required to reopen;
- Automatic lock out of the user ID when several erroneous passwords are entered. Events are logged and logs are reviewed on a regular basis;
- Utilizing firewall, router and VPN-based access controls to protect the private service networks and back-end-servers;
- Continuously monitoring infrastructure security;
- Regularly examining security risks by internal employees and third party auditors;
- Issuing and safeguarding of identification codes; and
- Role-based access control implemented in a manner consistent with principle of least privilege.
- Remote access to CARRIERX's services delivery network infrastructure is secured using two factor authentication mechanism.
- Access to host servers, applications, databases, routers, switches, etc., is logged.
- Access and account management requests must be submitted through internal approval systems.
- Access must be approved by an appropriate approving authority. In most cases, the approval for a request requires two approvals at minimum: the employee's manager and the role approver or "owner" for the particular system or internal application.
- Passwords must adhere to the CARRIERX password policy, which includes minimum length requirements, enforcing complexity and set periodic resets.
- Password resets are handled via CARRIERX ticketing system. New or reset passwords are sent to the employee using internal secure, encrypted email system.

Access Control to Use Specific Areas of Data Processing

Persons entitled to use the data processing system are only able to access Personal Data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied, modified or removed without authorization.

This is accomplished by:

- Employee policies and training in respect of each employee's access rights to the Personal Data;
- Users have unique log in credentials -- role based access control systems are used to restrict access to particular functions;

- Monitoring activities that add, delete or modify the Personal Data;
- Effective and measured disciplinary action against individuals who access Personal Data without authorization;
- Release of Personal Data to only authorized persons;
- Controlling access to account data and customer Personal Data via role-based access controls (RBAC) in compliance with the security principle of “least-privilege”;
- Internal segmentation and logical isolation of CARRIERX’s employees to enforce least-privilege access policies;
- Requirements-driven definition of the authorization scheme and access rights as well as their monitoring and logging;
- Regular review of accounts and privileges (typically every 3-6 months depending on the particular system and sensitivity of data it provides access to);
- Control of files, controlled and documented destruction of data; and policies controlling the retention of back-up copies

Availability Control

CARRIERX has implemented suitable measures to ensure that Personal Data is protected from accidental destruction or loss.

This is accomplished by:

- Global and redundant service infrastructure that is set up with full disaster recovery sites;
- Constantly evaluating data centers and Internet service providers (ISPs) to optimize performance for its customers in regards to bandwidth, latency and disaster recovery isolation;
- Situating data centers in secure co-location facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy;
- Service level agreements from ISPs to ensure a high level of uptime;
- Rapid failover capability; and
- Maintaining full capacity disaster recovery (DR) sites and annually testing DR centers by shutting down primary sites for at least 24 hours unless the product is running in active/active configuration.

Transmission Control

CARRIERX has implemented suitable measures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media.

This is accomplished by:

- Use of adequate firewall and encryption technologies to protect the gateways and connections through which the data travels;
- Sensitive Personal Data is encrypted during transmission using up to date versions of TLS1.2+ or other security protocols using strong encryption algorithms and keys;
- Certain types of customer Sensitive Personal Data and other confidential customer data (e.g. payment card numbers) are encrypted at rest within the system;
- Protecting web-based access to account management interfaces by employees through encrypted TLSv1.2
- End-to-end encryption of screen sharing for remote access, support, or real time communication;

- Use of integrity checks to monitor the completeness and correctness of the transfer of data.

Input Control

CARRIERX has implemented suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data processing systems or removed. This is accomplished by:

- Authentication of the authorized personnel;
- Protective measures for Personal Data input into memory, as well as for the reading, alteration and deletion of stored Personal Data, including by documenting or logging material changes to account data or account settings;
- Segregation and protection of all stored Personal Data via database schemas, logical access controls, and/or encryption;
- Utilization of user identification credentials;
- Physical security of data processing facilities;
- Session time outs.

Separation of Processing for Different Purposes

CARRIERX has implemented suitable measures to ensure that Personal Data collected for different purposes can be processed separately.

Documentation

CARRIERX keeps documentation of technical and organizational measures in case of audits and for the conservation of evidence. CARRIERX takes reasonable steps to ensure that persons employed by it and other persons at the place of work, are aware of and comply with the technical and organizational measures set forth in this document. CARRIERX, at its election, may make nonconfidential portions of audit reports available to customers to verify compliance with the technical and organizational measures undertaken in this Program.

Monitoring

CARRIERX does not access Customer Personal Data, except to provide services to the Customer which CARRIERX is obligated to perform, to monitor, analyze and improve the services, in support of the Customer experience, as required by law, or on request by Customer; CARRIERX has implemented suitable measures to monitor access restrictions of CARRIERX's system administrators and to ensure that they act in accordance with instructions received.

This is accomplished by:

- Individual appointment of system administrators;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for a reasonable period of time;
- Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and responsibilities.

Document History

version 1.0	01-01-2018	Initial revision	A.Okunev