OrgChart Now
Information Security Overview

OfficeWork Software LLC

Version 1.3
May 13, 2015

OrgChart Now Information Security Overview

Introduction

OrgChart Now is a SaaS (Software as a Service) product that allows customers to create organizational charts and workforce plans. A user's account typically contains employee data. Employee data can be either be uploaded or manually inputted into OrgChart Now. Employee data records may contain information that is considered confidential.

We know that one of your greatest concerns is the safety of your confidential data. OrgChart Now is designed from the ground up with security in mind. We follow industry best practices to ensure your data is safe.

Hosting Providers

All OrgChart Now servers are only hosted by providers that adhere to certain compliance standards and regulations. We require that our hosting providers are:

- SSAE 16/ISAE 3204 certified
- Safe Harbor certified
- ISO 27001 certified

Formerly known as SAS70 Type II, SSAE 16 and ISAE 3402 are the international service organizational reporting standards. These standards allow an auditor to assess the internal controls of hosted data center. ISAE 3402/SSAE 16 Type II SOC 1 reports are available to our customers and prospects upon request.

Safe Harbor is essentially a process for organizations in the US and EU that store customer data designed to prevent accidental information disclosure or loss. Companies certified under Safe Harbor must follow several guidelines regarding how data is collected, used, transferred and secured.

ISO/IEC 27001:2005 is the formal international security standard against which organizations may seek independent certification of their Information Security Management System (ISMS). It is intended to be used with ISO 27002:2005, a Security Code of Practice. ISO 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving ISMS, which is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

Physical Security

Access to each data center is controlled 24X7X365 by guards at the front entrance. Entrance to a hosting facility is only allowed when accompanied by an employee of the hosting provider.

Network Security

- Firewalls - All servers are protected by state of the art firewall technology to prevent unauthorized network access to servers and equipment.
- Intrusion Detection - Intrusion Detection and Prevention appliances are used to track and prevent unauthorized system access.
- SSL – Https is used for network connections to all servers to protect data in transit.

Server Security

All servers are hardened using industry standard guidelines as applicable. Passwords are changed on a periodic basis. All customer passwords are one way encrypted when at stored.

Information Security

All our employees and contractors receive information security training on an annual basis to ensure that they are aware of all information security related policies and procedures. Other training sessions are conducted on an ad-hoc basis as need arises.

Data Access

- Employee Access Control - A small group of designated employees are given access to customer data on an as needed basis. Access is granted and revoked as necessary by senior personnel.
- Customer Access - Customer is solely responsible for granting/revoking access to their employees/agents. Customer is responsible for making sure appropriate controls are in place for granting access privileges to their employees and contractors.

Data Retention

- Discontinued Usage - If a customer decides to discontinue usage of OrgChart Now, we will retain the customer data for a period of ninety (90) days. At that time we reserve the right to purge that customer's data from all systems. The customer can submit a written request that all data be purged immediately. We will purge data within ten (10) business days of a written request.
- Extended Retention - A customer can submit a written request to retain customer data for a longer than ninety days; however, this may result in additional storage fees to the customer.

Data Destruction

- Decommissioned and Repurposed Equipment - When equipment is decommissioned or repurposed, industry standard techniques are used to fully erase data from any attached storage media.
- Hard Copy Destruction - Hard copies of customer data are sometimes created in order to resolve a support ticket. Employees are trained to shred hard copies of customer data as soon as an issue is resolved.
- Downloading of Customer Data by Employees - If customer data must be downloaded to resolve a customer issue, the data can only be downloaded to designated servers. Employees are trained to perform a "deep delete" of the data as soon as an issue is resolved.
- Data Destruction Certificate - We will provide a data destruction certificate within ten (10) business days of a written request from customer.

Customer Guidelines

Although our systems are secure, we recommend that customers should avoid loading data elements that do not pertain to their business needs. For example, data elements relating to identify theft (e.g. Credit card information, bank account or financial account numbers, driver's license numbers or any health related records) should be avoided unless required by customer use case.

Data Ownership

Customer is the sole owner of their data. We acknowledge that customer data cannot be used for any purposes not expressly approved by customer.

Data Classification

Customer data is classified into three categories:

- Public – Customer data can that can be posted on public website
- Official Use Only – Customer data that can be used by us for business purposes (e.g. email campaigns or sales calls)
- Confidential – Customer data that is only accessible on an "as needed" basis in support of customer request (professional services or technical support).

All customer data stored in OrgChart Now is considered Confidential and is treated as such.

Data Segregation

We segregate customer data to ensure unauthorized access by another customer cannot occur. Segregation is achieved using industry standard database and file systems mechanisms.

Data Requests

At any time customer can request an electronic copy of any of their data. Customer must provide the request in written form and request must be signed by a corporate officer. The request must also contain specific delivery instructions for the requested data.

We will provide the data within ten (10) business days of this written request. A fee may be charged to customer based on the complexity of the request.

Testing Guidelines

In the event customer data is required for resolving an issue or testing a new software release, the data must be made anonymous before moving to development or test systems.