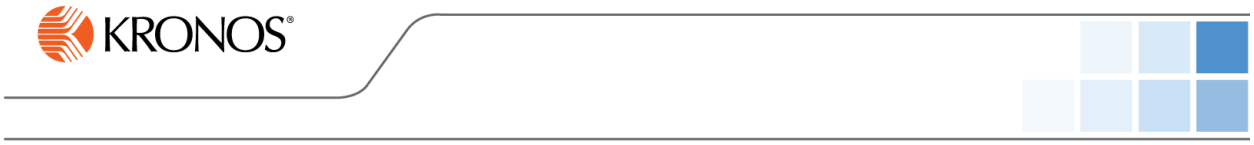


Service Organization Control (SOC) 3 Report

# Description of the SaaShr Infrastructure and Application Services System relevant to Security, Availability and Confidentiality for the period October 1, 2014 to September 30, 2015

## Table of Contents

Ernst & Young, LLP
200 Clarendon Street
Boston, Massachusetts 021116

Tel: +01 617 266 2000
Fax: +01 617 266 5843
ey.com

Building a better working world

## Report of Independent Accountants

To the Management of Kronos Incorporated:

We have examined management's assertion that Kronos Incorporated (Kronos), during the period October 1, 2014 through September 30, 2015, maintained effective controls to provide reasonable assurance that:

- the SaaShr Infrastructure and Application Services System was protected against unauthorized access, use, or modification
- the SaaShr Infrastructure and Application Services System was available for operation and use, as committed or agreed
- information within the SaaShr Infrastructure and Application Services System designated as confidential is protected as committed or agreed

based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Kronos' management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Kronos' relevant security, availability and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, Kronos' management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

Ernst & Young LLP

Ernst & Young LLP
October 30, 2015
Boston, Massachusetts

## Report by Management on the Controls over the SaaShr Infrastructure and Application Services System based on the AICPA/CICA Trust Services Principles and Criteria for Security, Availability and Confidentiality

Kronos Incorporated ("Kronos") maintained effective controls over the security, availability and confidentiality of its SaaShr Infrastructure and Application Services System to provide reasonable assurance that for the period October 1, 2014 to September 30, 2015:

- the SaaShr Infrastructure and Application Services System was protected against unauthorized access, use or modification;
- the SaaShr Infrastructure and Application Services System was available for operation and use, as committed and agreed; and
- information within the SaaShr Infrastructure and Application Services System designated as confidential is protected as committed or agreed;

based on the American Institute of Certified Public Accountants' TSP Section 100, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Our attached System Description of the SaaShr Infrastructure and Application Services System summarizes those aspects of the SaaShr Infrastructure and Application Services System covered by our assertion.

The Management of Kronos Incorporated

October 30, 2015

# System Description of the SaaShr Infrastructure and Application Services System

## Background

Kronos Incorporated ("Kronos") is a global privately held company founded in 1977, based in Chelmsford, Massachusetts, serving organizations in more than 100 countries, including many Fortune 1000 companies. These organizations use Kronos' time and attendance, scheduling, absence management, human resource, payroll, hiring and labor analytics applications. Kronos is a recognized leader in workforce management solutions that enable organizations to control labor costs and improve workforce productivity.

Kronos' workforce management solutions provide the complete automation and high-quality information Customers need to help control labor costs, minimize compliance risk, and improve workforce productivity. The Kronos solution can deliver continuous value only if it is available and managed properly over time. More Customers are choosing Kronos Cloud Services for hosting and deploying their workforce management solutions.

Kronos provides comprehensive hosting, maintenance, and support of the workforce management solution, including complete support of IT infrastructure encompassing computer hardware, operating systems, and database systems required to run Kronos application(s). This service includes other items such as:

- Server security and management
- Service pack installation
- Legislative update installation
- Software version installation
- Daily system and data back-ups

The SaaShr Infrastructure and Application Services System is comprised of the following six components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems and utilities)
- Data (files, databases, and tables)
- People (developers, operators, users and managers)
- Procedures (automated and manual)
- Application (solutions)

The following sections of this description define each of these six components comprising the SaaShr Infrastructure and Application Services System.

## Infrastructure

The infrastructure supporting the SaaShr environment all exists in a modular environment comprised of "pods." Each pod is bordered by redundant firewall technology, which is responsible for traffic policing and policy enforcement both in and out of the pod. Infrastructure servers, running Windows Server 2008 are authenticated/ authorized through Active Directory membership, group policy enforcement and public key cryptography. Each pod consists of multiple redundant application servers running on Windows Server 2008 and multi-tenant Microsoft SQL databases. Customer specific configurations and data are segmented logically within the Microsoft SQL Server database.

Kronos contracts with an industry recognized data center, Carpathia, which provides data center space, power and connectivity, as well as other managed services as discussed below for the infrastructure

supporting the SaaShr environment. The data center is a sub-service organization to Kronos. As part of the continuous monitoring program, Kronos reviews a copy of the most recent independent attestation report and monitors the services delivered by Carpathia.

Effective March 1, 2015, Kronos began using the existing US based SaaShr infrastructure housed in Dulles, Virginia to support their Australian (AU) instance of the SaaShr application. All processes and controls, as described below, were implemented for the Australian application instance prior to any customers being implemented in the environment.

Beginning October 13, 2014, Kronos' controls described within this description began to be implemented for the European Union (EU) instance of SaaShr housed in Amsterdam, Netherlands. As of July 1, 2015, the implementation of the processes and controls, as described below, was completed.

This report does not cover the application layer granting logical access to Customers' employees. The business office of SaaShr located in Branchburg, New Jersey houses physically secure servers, referred to as TRANZ servers, which pass through time punch entries directly to the SaaShr application.

## Software

The applicable software supporting the SaaShr environment only includes various utilities that are used by Kronos in managing and monitoring the environment. These utilities include items such as backup software, patch management, anti-virus and database management. Access to and use of these utilities is restricted to appropriate Kronos personnel.

## Data

Customer data is held in accordance with applicable data protection and other regulations set out in Customer contracts and limits access to electronically held Customer data on a need to know basis. Customer data is held in a SQL database technology and is managed by the Hosting Operations department. Data in transmissions are encrypted using Secure Socket Layer (SSL) sessions. Access to Customer data is limited to authorized and appropriate Kronos personnel, and is granted in accordance with system security administration policies.

## People

The following functional groups within Kronos are responsible for supporting the SaaShr Infrastructure and Application Services System:

- Product Engineering – This group designs, implements, tests and delivers features and service releases.
- Information Technology – This group provides architecture leadership for the underlying infrastructure that supports SaaShr and maintains the continuous monitoring program of the system.
- Hosting Operations – This group provides architecture leadership and is responsible for all aspects of running the production infrastructure, software and applications.
- Global Support – This group provides operational and Customer management support directly to Customers using the SaaShr application.
- Service Delivery & Support – This group provides pre-sales and implementation support to new and existing Customers.
- Sales, Technical Presales, Sales Operations, Marketing, Human Resources and Finance – Groups that provide overall corporate functions.

## Procedures

Kronos has documented policies and procedures that support the management, operations, monitoring and controls over the SaaShr Infrastructure and Application Services System. Specific examples of relevant policies and procedures include, but are not limited to, the following:

- Policy management and communication
- System security and administration
- Computer and network operations
- Data classification and confidentiality
- Service infrastructure management and administration
- Backup management and processing
- Monitoring and event correlation
- Vulnerability management
- Change management, including release to production processes

## Application

The SaaShr application is designed, deployed and maintained by Kronos resources to be delivered to Customers using the public internet. The software development life cycle includes releases first developed in a development environment, quality tested in a test environment and then promoted to production. Developers do not have direct access to change production resources.

The SaaShr application is a workforce management suite that is compiled from the following modules: Human Resources (HR), Payroll, Time and Labor Management, Leave, Accruals, Compensation, Scheduler, and Affordable Care Act (ACA). The solutions can be utilized individually, as a complete suite, or in conjunction with other third party applications, content and services. The Partners have the flexibility to choose what they would like to purchase in order to meet the unique needs of their organization.

Once a new contract is signed between Kronos and a Partner, Kronos Global Support opens a new ticket in the application ticketing system. Kronos Global Support then creates the Customer's company within the application based on the services and features purchased by the Partner in the contract. If an existing Partner wishes to enable additional features in the application, the Partner can do so at any time.

Once a Partner company is created, the Partner can configure and customize the application, including any specific reports required by the Customer. A Partner creates Customer companies, configures the application per Customer needs, and enables standard features as needed based on contracts with the Customer. Kronos only makes changes to Partner and/or Customer environments at Partner's request in the event a Partner is unable to complete the task themselves. As the application is highly customizable, any input, processing and output field configurations are also determined by the Partner and their Customer. The underlying application code logic, which forms the basis of the results of calculations displayed by the application, is subject to the Kronos change management controls to facilitate complete and accurate calculations of data.

## Sub-service Organizations

Kronos utilizes Carpathia ("sub-service organization") to provide data center hosting services, including physical security and environmental safeguards, to support SaaShr. It is expected that the sub-service organization has implemented the following controls to support achievement of the associated criteria:

| Criteria Reference | Expected Sub-Service Organization Controls |
|---|---|
| CC5.5 | Access to the data center is restricted to authorized employees and contractors through the use of card readers and other systems (e.g. hand readers). |
| | Visitors to the data center are required to sign a visitor log. |
| | Physical access to the data center facilities is restricted to appropriate personnel who require such access to perform their job functions. |
| | Administrative access to the card system and other systems (e.g. biometric readers) is limited to authorized and appropriate personnel. |
| | Camera surveillance of the data center is monitored and retained for a period of time. |
| A1.2 | Environmental safeguards at the data center facilities are designed, implemented, operated, and maintained, including the following:<br>• Fire detection and suppression systems<br>• Climate, including temperature and humidity, control systems<br>• Uninterruptible power supplies (UPS) and backup generators<br>• Redundant power and telecommunications lines |

## Complementary User Entity Controls

In designing the System, Kronos has contemplated that certain controls would be implemented by user entities to achieve the applicable trust services criteria supporting the System, which were communicated to user entities through the contract acceptance process. The complementary user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities.

- User entities are responsible for determining that the functionality within SaaShr system meets their requirements and notifying Kronos timely with any required changes or enhancements.
- User entities are responsible for managing (i.e., user provisioning, user de-provisioning, access reviews) and configuring application logical access (i.e., password settings, multi-factor/two-factor authentication) to ensure that access remains restricted to authorized and appropriate personnel.
- User entities are responsible for communicating security, availability and confidentiality commitments and responsibilities to their internal and external users accessing data within the System and providing users with the resources necessary to fulfill their commitments and responsibilities.
- User entities are responsible for adequately securing and disposing of any system output provided by the System.
- User entities are responsible for securing transmissions of data to Kronos, which includes transmissions from non-Kronos middleware, and informing Kronos of any necessary changes to the System.
- User entities are responsible for implementing processes and controls to prevent and detect unauthorized or malicious software and unauthorized access to the system or activity.
- User entities are responsible for approving and validating the appropriateness (and maintaining the confidentiality) of data provided to Kronos and any changes to that data.
- User entities are responsible for configuring their customers on the application, including verifying the accuracy and completeness of changes made by their system administrators or Kronos on behalf of the user entities.
- User entities are responsible for reviewing changes to their data to ensure that all changes are appropriate and authorized.
- User entities are responsible for reviewing notifications from Kronos of changes to the SaaShr environment and communicating any concerns to Kronos.
- User entities are responsible for ensuring their systems are in compliance with regulatory requirements and state laws, any specific requirements should be communicated to Kronos in a timely manner.
- User entities are responsible for communicating any identified incidents impacting the security, availability or confidentiality of the system to Kronos on a timely basis.
- User entities are responsible for reviewing application audit trails and notifying Kronos of any discrepancies or unauthorized activity.