

Software as a Service (SaaS) Requirements

Introduction

Software as a Service (SaaS) is a software service model where an application is hosted as a service provided to customers across the Internet. By eliminating the need to install and run the application on the customer's own servers and network, SaaS alleviates the customer's burden of software maintenance, ongoing operation, and support. While the technical needs for servicing the application is no longer needed, the burden of meeting CPCC's technology standards, security standards, service standards, and regulatory policies must be held. This document provides the basis of these requirements.

General Services

Authentication Environment

CPCC has a strict policy requiring SaaS vendors to provide authentication through CPCC's authentication solution. Service providers must be able to interface with the current version of CAS (Central Authentication Service) utilized at CPCC. CAS is an open source authentication solution that was originally developed Yale University and is now a JA-SIG project. CAS provides a single-sign on authentication system.

Additional information may be obtained through <http://www.ja-sig.org/products/cas/>. Information regarding the specific version of CAS supported at CPCC can be found at www.cpcc.edu/web-services.

In the event that a provider is not able to interface with CAS, a letter of exception must be approved by CPCC ITS.

Service Authorization

Services provided by the SaaS must provide authorization capabilities internally within the application. These services must be documented and provided to ITS along with all information stored by the SaaS provider related to individuals, groups, and authorization schemas.

Reporting Services

In the event that regular data extraction is not available for the use of developing reports with CPCC reporting solutions, then a description of available reporting services must be provided. Details with regards to documentation and training should be included.

Customization Capabilities

Services provided by the SaaS may not meet all the requirements of CPCC. Therefore, customizations may be required to meet these requirements. However, customizations may be provided in various ways and with limitations. Customizations should be categorized as the following and the requirements must be met –

1. Configuration: pre-determined options available to CPCC with the ability to easily modify. Typically, provided through either a configuration file or settings in a database table.
 - a. Requirement:
 - i. It must be clear as to when changing a configuration after the services has been started can potentially lead to a problem with service or with the history of the data.
2. Fixed Customizations: pre-determined and limited features CPCC can customize either by modifying an existing file, new file, or through an application programming interface (API).
 - a. Requirements:
 - i. Documentation detailing the ability to customize the file or about the API.
 - ii. Information regarding how future upgrades may impact these customizations.
3. Open Customizations: source code is either partially or fully available for CPCC to customize the code as needed.
 - a. Requirements
 - i. Documentation regarding the code available for customization.
 - ii. Documentation regarding coding methodology, if one exists.
 - iii. Information regarding how future upgrades may impact these customizations and equivalent documentation if code-merge is required.
4. Change-Request Customizations: customizations that has been reviewed and approved between CPCC and SaaS that will be conducted and maintained by SaaS.
 - a. Requirements
 - i. Documentation regarding the process to request customizations.
 - ii. Cost estimate for requested customizations.
 - iii. Information regarding how future upgrades may impact these customizations.

Customizations may be a great benefit to CPCC in meeting most, if not all, the specific needs. However, it must be weighed against the cost of maintenance, especially if it leads to potential downtime of services.

End User Training

Training provided to the College should be reviewed in a partnership with ITS to ensure compliance with the College's Information Technology Standards.

Service Level Agreements SLAs

Agreements regarding software and/or applications should be review in conjunction with ITS to ensure compliance with the College's Information Technology Standards.

Data Storage

All data stored by the SaaS provider must be secured in a manner which prevents unauthorized access from internal and external parties. If possible, data should be encrypted.

Data Storage Location

The SaaS provider must locate all stored data in the United States of America unless given express permission by CCCC.

Backups

The SaaS provider must provide proof of their Business Continuity / Disaster Recovery plan including details on backups and retention periods. Backups that are stored offsite must be encrypted.

Migration Strategies

Migration strategies are required in preparation of any event requiring the transition of the data to a different SaaS or internally to CCCC for continued service. If no such strategy is available, then procedures and documentation, including ER diagrams or equivalent diagrams, for a complete extraction of data is required.

Data Retention / Release

In the event of termination of contract, all data will be returned to CCCC ITS in a suitable standard format and wiped from the SaaS provider's systems. This may also include the removal of backup data from tapes if the retention period is too long for aging to occur naturally.

The SaaS provider must adhere to any and all data retention / removal policies stipulated by the College.

System Requirements

Browser Requirements

Any online services provided are required to be compatible with modern common browsers including: Firefox 3.x, IE 7.x, IE8.x, and Safari 5.x. Any online service should also pass the w3.org validator test (<http://www.w3.org/QA/Tools/>) and be compatible with federally regulated accessibility standards (Section 508, <http://www.section508.gov/>).

Client Requirements

As a rule any service provided online should not require the use of a "client" installed component (e.g. activeX, java). If a client is required for the service the provider must agree in writing to maintain client compatibility and must provide in writing any data that will be transmitted using the client component.

Any client software must be compatible with Windows XP (service pack 2 and above), Windows Vista (all versions), and Windows 7 (all versions). It is highly recommended that client components also be compatible with the Mac OSX platform.

SaaS providers must agree to periodic audits of transmitted information by both CCCC ITS and state auditors as requested.

Data Transfer

All data transfers will be encrypted using 128bit (or higher) SSL for HTTP traffic and SSH version 2 for any batch or real-time non-http transfers. Furthermore, SSL certificates must be signed by a trusted third party; no self-signed certificates will be considered.

Inbound or outbound batch transfers must occur between endpoints that have a firewall policy that allows only the two endpoints to exchange data.

DNS / Domain Registration

Where possible, all SaaS provided services will use the following format: *saas.cpcc.edu*

The service name will be negotiated between CPCC ITS, the SaaS provider, and the CPCC requesting entity. The SaaS provider will provide CPCC with the IP(s) to resolve the address and they will be configured on CPCC's DNS servers. If changes are made afterwards, they must be communicated to CPCC ITS in a timely manner to prevent service interruptions.

If a new domain is to be registered instead, it will be procured and administered by CPCC ITS.

Email Requirements

CPCC will as a rule not allow the SaaS provider to 'spoof' its domains in the envelope sender. Other headers (From, Reply-To, etc.) must be used instead.

In certain circumstances, spoofing will be allowed but only if mail from the SaaS provider is directed to CPCC staff or faculty and never to non-CPCC entities or CPCC students. In such cases, a small number of MTA IP addresses will be provided to CPCC ITS for use in white-listing. If changes are made afterwards, they must be communicated to CPCC ITS in a timely manner to prevent service interruptions.

In circumstances where email is directed to students, the SaaS provider must verify that they meet Google's Acceptable Use Policies.

Workstation Environment

Desktop applications should operate using current versions of Microsoft Windows and/or Apple Operating Systems.

Data Integration

Integration Requirements

SaaS solutions providing services that either require real-time data from the ERP system or update data into the ERP system must have an interface that have been developed with the Envision Toolkit or any other tools approved by Datatel. Any other interfaces, including the use of an integration broker, must have details disclosed to insure proper operations without compromising services, security, and corruption of data. These interfaces should be available for CPCC to review and properly maintain. In

the event that an integration broker is hosted by a third-party company, then all requirements apply to this company as well.

Enterprise Application Environment

The primary enterprise level application deployed and supported at Central Piedmont Community College (CPCC) is the Educational Enterprise Resource Planning (ERP) system which includes the Student Information Systems, Human Resource Management, and Financial Resource Management.

The current ERP system is Datatel, a product and service selected by the North Carolina Community College System (NCCCS). Datatel currently is deployed using a propriety language known as Envision which uses IBM's Universe package as the foundation. In addition to using Unibasic as part of the Universe package, Unidata is used as the primary database for Datatel.

While Datatel is the implemented ERP system, the Unidata database is the single source of data for the majority of information. In addition, to support other related systems, such as a Learning Management System (LMS), CPCC developed an Operational Data Store (ODS) using Microsoft SQL Server where data is stored through a locally developed ETL (Extract, transform, and load) tool. In addition, CPCC deployed several SOAP (Service Oriented Architecture Protocol) interfaces to allow for data extraction from the ODS.

Policies/Regulations

Data Ownership

Unless there is a written agreement between CPCC and the SaaS provider with regards to data ownership, all data is exclusively owned by CPCC and a written agreement is required if the SaaS provider will use the data other than the primary purposes of providing all agreed services. All data must be handled and secured according to the "Security and Data Protection" section.

Security and Data Protection

The following set of statements will be a component of any contract or other instrument that results from evaluation of responses to RFPs:

Vendor shall treat all data that it receives from Central Piedmont Community College (CPCC), or is otherwise exposed to within CPCC data systems, with the highest degree of confidentiality and in compliance with all applicable federal and state laws and regulations and University policies. Vendor shall employ commercial best practices for ensuring the security of all CPCC electronic and paper data accessed, used, maintained, or disposed of in the course of Vendor's performance under this Agreement. Vendor shall only use such data for the purpose of fulfilling its duties under this Agreement and shall not further disclose such data to any third party without the prior written consent of CPCC or as otherwise required by law.

Without limiting the foregoing, in the course of performing its duties under this Agreement Vendor MAY receive, or be exposed to, the following types of data: student education records; financial information as that term is defined in the Financial Modernization Act of 1999; protected health information as that term is defined in the Health Insurance Portability and Accountability Act; and various items of personal identifying information including but not limited to Social Security Numbers, credit card numbers, financial account numbers and corresponding security or access codes and passwords, drivers license numbers, and Indiana state identification card numbers. Vendor shall employ sufficient administrative, physical, and technical data security measures to meet the requirements under the specific federal and state laws applicable to those data, including but not limited to:

- Student Education Records: The Family Education Rights and Privacy Act (FERPA), 20 USC 1232g et seq., and related regulations at 34 CFR Part 99;
- Financial Information including credit card and financial account numbers: The Financial Modernization Act of 1999, 15 USC 1681 et seq.; the Safeguards Rule at 16 CFR Part 314; and North Carolina GS_75-65.
- Protected Health Information: The Health Insurance Portability and Accountability Act ("HIPAA"), 42 USC 1320d-2 (note); implementing privacy and security regulations at 45 CFR Parts 160 and 164, and related agency guidance; and the terms of any Business Associate Agreement or LOS agreement between CPCC and Vendor;

Immediately upon becoming aware of a breach of the Vendor's security that reasonably may have resulted in unauthorized access to CPCC data, Vendor shall notify CPCC and shall cooperate fully with CPCC's investigation of and response to the incident. Except as otherwise required by law, Vendor shall not provide notice of the incident directly to the persons whose data were involved, without prior written permission from CPCC.

Vendor acknowledges and agrees that CPCC is subject to North Carolina's Open Records law, and that disclosure of some or all of confidential information provided pursuant to this Agreement, or the Agreement itself, may be compelled pursuant to that law. CPCC agrees that, upon receipt of a request for confidential information made pursuant to the North Carolina Open Records law, it shall "a) promptly notify Vendor of the fact and content of the request, b) consult with Vendor regarding any legitimate basis on which it might resist or narrow its response to the request, and c) disclose only information that CPCC, in the opinion of its legal counsel, is legally compelled to disclose."

Further, CPCC has a robust and active technology security Office and program. The information at <http://www.cpcc.edu/its/faculty-staff/its-security> gives a further over overview of the laws mentioned above, and also outlines those security implementations considered by CPCC to be "best practices" for protection of sensitive institutional and personal data.

Regulatory Compliance

Along with the specified requirements for privacy and security of information as described in the "Security and Data Protection" section, CPCC will minimally request a copy of the Statement on Auditing Standards No. 70 (SAS 70) report.

Appendix A – Table of current versions supported

Client (Desktop)	Windows	Windows XP (SP3) Windows 7
	Mac	OS X 10.3, 10.4, 10.5, 10.6
Browsers	Internet Explorer	Version 7, 8
	Firefox	version 3.x.xx
	Safari	version 5.x.xx