# Cloud Service (SaaS) Acquisition Checklist

Version Updated: 12/2020

This document serves as a guide to assist Finance, Legal, Purchasing, IS&S, and campus units in developing a professional approach for the acquisition and maintenance (aka. life cycle) of cloud solutions or Software as a Service (SaaS). It is not meant to be a guideline for product evaluation or selection. This policy has been approved by the Berea College Administrative Committee in 2017, which mandates that no IT services, software purchases, or renewals will be made without a completed and fully approved checklist.

Please note that Appendix A is a glossary of terms that will help you understand what terminologies mean and who to contact. Appendix B contains contact information for Berea employees who you may consult with if you need assistance in completing this checklist. It is essential that the requestor complete the checklist and include: appropriate documentation, approvals, and signatures. Some of the documentation should be obtained from the vendor and can be sent to IS&S in electronic format. Once completed, please submit check list to: IS&S, CPO 2208, ATTN: Info Security Officer and by email to #IT-Checklist@berea.edu

Vendor Name: _____ Product: _____

Department/Division: _____

Requestor(s) (print, sign and date): _____

AC member (print, sign, and date): _____

**Overview**

Please provide a general description of what this product does and who will be using it.

## 1. General

1.1. Please list one or more "service owner" (aka, technical or administrative point of contact) that can provide necessary Berea College end user support and serve as the main contact for issues with vendor. **IMPORTANT: The "service owner" is responsible for maintaining the latest security updates and patches on the application.**

- *Specify the names of individual(s) who will be the service owner(s) at Berea College:*

  _____

1.2. The service should have 3rd party support arrangement.
*(Attach the vendor's Service Level Agreement (SLA) or contract for review.)*

1.3. The vendor should provide technical documentation as part of their service.
*(Attach this documentation and/or the web url for review.)*

1.4. Is there a need for any Network Control changes for this product? (Ports opened, DNS changes/additions, Firewall rules, etc)

____ No _____ *Initial Here* _____ *Date Here, skip to 1.5*

____ Yes (continue below)

Please note that there is a minimum of 8-weeks lead time for integration.

- *Type of Network Control change*_____
- *Date needed*_____
- *Please attach information required for changes (Port #'s needed, etc)*

*Reviewed by IS&S Net/Infra Director (signature)*_____

1.5. Is there a need for the software to interface to Banner or MyBerea to obtain data?

____ No _____ *Initial Here* _____ *Date Here, skip to 1.6*

____ Yes (continue below)

Please note that there is a minimum of 8-weeks lead time for integration.

- *Type of Banner data needed*_____
- *Date needed*_____
- *Please attach a summary of data and/or transaction needs and protection plan.*

*Reviewed by IS&S Enterprise Director (signature)*_____

1.6. Is there a need for single sign-on (SSO) (ie. using Berea username and password)

____ No _____ *Initial Here* _____ *Date Here, skip to 2.1*

____ Yes (continue below)

Please note that there is a minimum of 4-weeks lead time for integration.

- *Type of integration needed*_____
- *Date needed*_____
- *Please attach a brief summary.*

*Reviewed by IS&S Net/Infra Director (signature)*_____

## 2. Data Protection & Access Security

To access and/or store sensitive or regulated data, permission must be obtained from the appropriate data steward(s). Please refer to the attached Glossary of Terms for categories, definitions, and responsible units.

2.1. Any regulated data needed (please circle)?

*HIPAA FERPA PCI PII PHI N/A*

- *If yes, please attach necessary approval(s) from the appropriate stewards.*

- *If "N/A", please initialize _____ Initial Here _____ Date Here, skip to 2.2*

2.2. Any sensitive data needed (please circle)?

*Intellectual property donor info financial HR Legal Credentials N/A*

- *If yes, please attach necessary approval(s) from the appropriate stewards*
- *If "N/A", please initialize _____ Initial Here _____ Date Here, skip to 2.3*

2.3. If College regulated or confidential data will be stored by the application, please attach vendor's SOC 1 or 2 or SSAE compliance documentation.

*_____ Attached*

*_____ N/A _____ Initial Here _____ Date Here, skip to 2.4*

2.4. If College regulated or confidential data are to be stored/used by the service, it is required that all communications and storage be encrypted.

- *If this is not applicable, _____ Initial Here _____ Date Here, skip to 2.5*
- *If yes, please attach technical documentation for communication (URL is acceptable)*
  *Reviewed by IS&S (signature and date)_____*
- *Attach technical documentation for data storage encryption. (URL is acceptable)*
  *Reviewed by IS&S (signature and date) _____*

2.5. Is the service mandatory for students or employees? If yes, section 508 (ADA) compliance attestation (VPAT) should be attached and will be reviewed by IS&S and DAS.

- *If this is not applicable, _____ Initial Here _____ Date Here, skip to 2.6*
- *If yes, please attach completed VPAT (from the vendor).*
  *(If the service is mandatory and no VPAT is available, or if the VPAT is not acceptable, please acknowledge that there is a chance the purchase will not be approved, unless acceptable accommodations are made with the approval of DAS. Contact Lisa Ladanyi for additional help.)*

2.6. Will this service store any data relating to an individual that is affiliated with Berea College?

- *If this is not applicable, _____ Initial Here _____ Date Here, skip to 2.7*
- *If yes, please attach vendor information on GDPR Compliance (from the vendor). See GDPR under Appendix A for more details. This compliance is not a US compliance but one Berea College must meet as we have EU students, employees, donors, etc.*
  *Reviewed by IS&S (signature and date) _____*

2.7. Please provide local (Berea College) user access control and management for this solution.

- *Specify required access types, who will have accesses, for how long, how often, and who will review annually (use attachment if necessary)*

_____

_____

_____

## 3. Contract

3.1. Does the contract or term & conditions includes start and end dates, renewal, notification, and breach of contract? *Yes No*

3.2. Berea College reserves the right to request the vendor to return and properly destroy any College data upon contract termination. Can this be done? *Yes No*

3.3. Does the service provides a way to perform periodic data backup and recovery? *Yes No*

3.4. Does the service allow for activity details and logs at fixed intervals? *Yes No*

3.5. Please provide documentation on data protection and privacy. ____ *Attached* ____ *N/A*

3.6. Please provide documentation on how the vendor will work with Berea College for troubleshooting or support requests? ____ *Attached* ____ *N/A*

3.7. Funding and renewal expenses has to be identified by the unit and approved by Finance.

- *Funding source:*

  _____

*Please be aware that SaaS Checklists are subject to an annual review process that may require additional information during the renewal process, in order to comply with current policy or regulation.

Vendor Name: _____ Product: _____

## Approvals (print name, signature and date)

PFE Director of Operations: _____ ____/____/____
(Only for PFE Requests)

Information Security Officer: _____ ____/____/____

Chief Information Officer: _____ ____/____/____

Internal Auditor: _____ ____/____/____

Controller: _____ ____/____/____

Finance: _____ ____/____/____

**Comments**

_____

_____

_____

_____

_____

# Appendix A: Glossary of Terms

**Access control:** This refers to what rights to access to files or services are being requested for a user or a group of users, ie. who can do what and when.

**ADA:** Americans with Disabilities Act. The ADA is a civil rights law that prohibits discrimination against individuals with disabilities in all areas of public life and gives civil rights protections to individuals with disabilities similar to those provided to individuals on the basis of race, color, sex, national origin, age, and religion. For more information, please contact DAS (see below).

**Credentials:** This typically refers to username and passwords and/or tokens, which require special protection. The steward for Berea College enterprise credentials is Information Systems and Services.

**Cloud Service:** a broad category that encompasses the myriad IT resources provided over the Internet. Any service that is accessed over the Internet (mostly thru browsers or phone apps) that is not hosted on a College server is considered a cloud service.

**DAS:** Berea College Disability and Accessibility Services department.

**FERPA:** The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The steward for Berea College FERPA data is the Registrar.

**GDPR:** The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It also addresses the export of personal data outside the EU

**HIPAA:** The Health Insurance Portability and Accountability Act of 1996 is United States legislation that provides data privacy and security provisions for safeguarding medical information. The steward for student HIPAA data is the Registrar, and for employee HIPAA data is Human Resources.

**Intellectual property:** Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. The steward for all Berea College IP is the Dean of Faculty.

**IS&S:** Berea College Information Systems and Services department. The Berea Chief Information Officer oversees IS&S.

**PCI:** The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. Anything that deals with credit cards, processing credit card transactions, or anything related to credit cards must be PCI compliant. The main steward for all Berea College PCI data is the Controller.

**PHI:** Protected Health Information. Under US law, any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history. The main Berea College steward for student PHI data is Registrar, and for employees Human Resources.

**PII:** Personally Identifiable Information is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII. The main Berea College steward for student PII data is Registrar, and for employees Human Resources.

**SaaS:** Software as a service is a software or service that has licensing and delivery model based on a subscription basis and is hosted in a datacenter offsite. See also *"Cloud Service"*

**Service Owner:** The "Service Owner" is the person who will be accountable for a specific service or software application regardless of where the technology components reside (onsite or in the 'cloud') - this person will serve as the main contact for Berea College when setting up or providing support to the service or software application.

**Service Provider:** Any organization or vendor that provides a service or software to the College. An example would be Microsoft, who provide software, cloud services, and technical support to the College. See also "SaaS" and "Cloud Services."

**Single Sign-on:** *Single sign-on* (SSO) refers to the ability of a user to login to a service that using their College username and password. It permits a user to use their College credentials to access multiple applications.

**SOC:** Service Organizational Controls. This refers to the established plan of action that a service provider has established for how they will react in the event of a breach of access to stored information. See also *"SaaS"* and *"Cloud Services"*

**SSAE:** Also called "Statement on Standards for Attestation Engagements 16" requires service companies to report on compliance controls by providing a written assertion of compliance for the services provided as well as any operational activities that affect the service's customers. See also *"SOC"*

**SSO:** See *"Single Sign-on"*

**VPAT:** A VPAT (Voluntary Product Accessibility Template) is a vendor-generated statement that provides relevant information on how a vendor's product or service claims to conform to the Section 508 Accessibility Standards for Electronic and Information Technology. See also *"ADA"*

# Appendix B: Contact Information

| | | |
|---|---|---|
| Phillip Logsdon, | Chief Information Officer, logsdonp@berea.edu | |
| Sara Clements, | Controller, | clementss@berea.edu |
| Kevin Hall (PFE), | Director of Operations, | hallk@berea.edu |
| Rozella Shell, | Internal Auditor, | shellr@berea.edu |
| Jeremy Sutcliffe, | Information Security Officer, | sutcliffej@berea.edu |