SaaS / Third-Party Data Handling Procedure

Issue Date: 08/08/2018
Expiration Date: N/A
Category: ITS Internal Procedure

1.0 – Background

The College understands the value provided by and occasional requirement to use third-party entities to provide hosted software-as-a-service (SaaS) offerings, and/or to utilize third-party entities in the collection, storage, and sharing of data (referred to hereafter as "data processing agents" or DPAs) related to College constituents. When well-vetted, these services can provide significant additional value to College constituents.

2.0 – Purpose

The purpose of this procedure is to ensure that proper consideration is given to the risks and benefits of any SaaS or DPA relationship before it is formalized and to routinely evaluate the effectiveness of the partnership and the value derived relative to the potential risk to the College.

3.0 – Procedure

PRIOR to evaluating a SaaS or DPA offering for use by the College, interested program areas must complete the following checklist and submit it to the CIO or CISO for review along with relevant details of the SaaS/DPA service. A "no" answer to any of the items may result in dis-consideration of the SaaS/DPA offering.

1. Does the service provide required functionality and/or features above and beyond those currently available via existing internal or third-party solutions?
2. Is the service provided by a reputable, stable business capable of supporting the integration and ongoing maintenance of the service within the College's environment?
3. If the service requires authentication by users, does it integrate with the College's Identity and Access Management (IAM) platforms (e.g. CAS and/or Shibboleth)?
4. Does the service maintain audit logs of access to the service and changes made within the offering? If yes, can those logs be exported manually or automatically (for example, to a SIEM tool)?
5. Does the service provide any redundancy and/or fault tolerance, and if not, do you have a plan should the service be unavailable for any period of time?
6. Does the service comply with all College policies and procedures?
7. Is the service ADA-compliant?
8. If the service is used for the collection, storage, or transmission of sensitive information (refer to "Yavapai College Data Classification Standard" – "DCS"), can the business guarantee compliance with the YC DCS and the College's "Media Protection Procedure"?
9. If integration support will be required from the Information Technology Services department, have you consulted with the appropriate individuals on resource allocation?

Yavapai COLLEGE

Once the above information is provided to the CIO or CISO, a review will be conducted promptly and written approval or rejection will be provided within two weeks (or more promptly if possible).

Appeals of non-approvals may be submitted to the program area Vice President for review and final adjudication.

4.0 – Non-Compliance

Any SaaS or DPA offering found to be in-use without prior written approval may be subject to immediate discontinuation.

5.0 – Auditing and Review

The CISO or CIO or their designees will work with all program areas annually to review use of SaaS/DPA services to confirm continued business utility and compliance with Information Security and Regulatory requirements. This process may also be used to identify unauthorized SaaS/DPA services.

6.0 – External Guidance/Reference

NIST 800-53r4: AC-20, AC-21; CSC: 13

7.0 – Revision History

Author	Date	Version	Reason
S. Hagan	08/07/2018	1.0	Initial Creation
S. Hagan	08/08/2018	1.1	Standardized terminology (DPA vs DCA)
S. Hagan	12/10/2018	1.2	Minor Updates (Grammar, Section 6)

8.0 – Inquiries

Direct inquiries about this procedure to:

Patrick Burns
Chief Information Officer – Yavapai College
E-mail: Patrick.burns@yc.edu
Voice: (928) 776-2055

Yavapai COLLEGE