Contents

Document Review Log 2
Purpose and Scope 2
Responsibilities 2
Policy 2
Selecting and Contracting for 3rd Party Services 2
References 4
Exhibits 5
Exhibit A - Draft Contract Language for 3rd party IT Services* 5
Definitions 5
Security and Accessibility-related Terms & Conditions 5

Document Review Log

Date Reviewed	Description of Changes
8/17/2023	Initial Draft approved by Senior Leadership Team

Purpose and Scope

This policy outlines security expectations and responsibilities for 3rd party partners and providers. It applies to any companies or individuals who provide or support Alvernia University ("AU") systems and applications, or who manage AU data. It also provides guidance to AU faculty & staff who contract these services.

Responsibilities

Title or Role	What They are Responsible For
Chief Information Officer	Maintains and Enforces this policy.
Senior Leadership Team, Legal and IT Team members	Ensure 3rd party providers and partners understand and execute their responsibilities, and incorporates this guidance in the product selection and contracting process.
3rd Party Partners and Providers	Ensure their systems and processes meet the minimum requirements outlined in this policy.

Policy

This policy is derived from the general IT Security framework outlined in **9.1000, IT Security and Governance**, and the specific IT controls defined in **9.3000, IT Security for IT Professionals**. It defines what should minimally be included when selecting and contracting 3rd party services, and how compliance should be monitored ongoing. Note, 3rd party contractors who provide IT maintenance services to AU hosted systems and applications must comply with 9.3000, IT Security for IT Professionals. For the purpose of this policy, a 3rd party partner or provider is defined as an organization that provides, hosts, or manages a system or application that performs business processes for AU and/or handles AU Internal or Confidential data.

Selecting and Contracting for 3rd Party Services

AU faculty & staff who select and contract for 3rd Party Services must use good faith efforts to work with the IT team to do the following as part of the selection process:

1) Identify the type and classification of the AU data to be carried by the 3rd party provider, as defined in **9.1000**.
2) Define the Confidentiality, Integrity, and Availability level for the system, as defined in **9.1000.**
3) Ensure the 3rd party system meets or exceeds the controls outlined in 9.3000 based on that definition.
4) Evaluate the risk of outsourcing the business process, and the overall security maturity of the 3rd party provider. An IT Team member shall be engaged to assist in this evaluation and perform technical due diligence.

Once the system has been selected, AU faculty & staff must use good faith efforts to work with the IT team to ensure the contract includes language that:

1) Clearly defines the AU information that is to be exchanged with, stored on, or processed by the 3rd party provider.
2) Requires compliance with AU controls. If the 3rd party is handling payment card information, this must include a requirement to be PCI compliant.
3) Defines minimum service level expectations in terms of availability and outlines the consequences.
4) Allows AU to monitor 3rd party compliance as necessary.
5) Addresses non-disclosure of AU Internal or Confidential data.
6) If the 3rd party is handling payment card information, requires the 3rd party provider to provide evidence that security incident response procedures are in place.
7) Addresses the return or destruction of data in the event of contract termination, including what happens in the event of a business failure of the 3rd party. This should include the return or destruction of data when no longer required to support the outsourced activity.
8) Explicit protection for AU Intellectual Property, including preservation of copyright and patent, as applicable.
9) A Source Code Escrow shall be required for all systems that are essential to AU's business. This requirement can be waived depending on the relative importance of the system.
10) If the 3rd party is handling payment card information, requires the 3rd party provider to provide evidence that IT configuration management and change control procedures are in place.
11) If the service provided is a multi-tenant service (the system is used by multiple customers, not just AU), there should be particular language and controls defined for protecting AU information from being exposed to other customers.
12) For service providers that handle payment card data, the contract should clearly define which PCI DSS requirements are managed by the service provider, and which by AU. *Note: This is PCI Requirement 12.8.5.*

In addition, if the 3rd party provider is handling payment card information (credit card/debit card information), they must have implemented a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:

• Firewalls

• IDS/IPS

• Identity Management

• Anti-virus

• Physical access controls

• Logical access controls

• Audit logging mechanisms

• Segmentation controls (if used)

The IT team will review the compliance of service providers who handle cardholders' data at least annually. Service providers will be required to provide a current Letter of Attestation and supporting evidence (a PCI Self-Assessment Questionnaire or 3rd party audit summary).

Contracted IT Systems that provide web-based interfaces for prospective or current students must also meet the standards outlined in 9.5000 for Web Accessibility.

All contracts should be reviewed by Legal prior to execution. The table below is a matrix that shows the required controls based on the confidentiality, integrity, and availability level of the system. Exhibit A contains draft contract language for use in 3rd party contracts.

9.3000 Control Family	Level at which Required Confidentiality	 Integrity	 Availability
3.1 Access Control	Low	Low	Low
3.2 Awareness and Training	Medium	Medium	Medium
3.3 Audit and Accountability	Medium	Medium	N/A
3.4 Configuration Management	Medium	Medium	Medium
3.5 Identification and Authentication	Low	Low	N/A
3.6 Incident Response	Medium	Medium	Medium
3.7 Maintenance	Medium	Medium	Medium
3.8 Media Protection	Medium	Medium	N/A
3.9 Personnel Security	Medium	Medium	Medium
3.10 Physical Protection	Medium	Medium	Medium
3.11 Risk Assessment	Medium	Medium	Medium
3.12 Security Assessment	Medium	Medium	Medium
3.13 System and Communications Protection	Medium	Medium	N/A
3.14 System and Information Integrity	Medium	Medium	Medium

References

This section contains any 3rd party standards, guidelines, or other policies referenced by this policy.

1. 9.1000, IT Framework and Governance
2. 9.3000, IT Security for IT Professionals
3. 9.3400, IT Configuration Management
4. 9.3600, IT Security Incident Response
5. SANS Institute InfoSec Reading Room, A Security Guide for Acquiring Outsourced Service, https://www.sans.org/reading-room/whitepapers/services/security-guide-acquiring-outsourced-service-1241
6. Payment Card Industry (PCI) Data Security Standard, v3.2
7. Cloud Standards Customer Council, Public Cloud Service Agreements: What to Expect and What to Negotiate Version 2.0.1, http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf
8. Lexis Practice Advisor Journal, Drafting and Negotiating Effective Cloud Computing Agreements, 11-30-2015, https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2015/11/30/drafting-and-negotiating-effective-cloud-computing-agreements.aspx

Exhibits

This section contains links to any documents that are required to be used by the policy. Examples would include required forms or links to internal websites or systems required to implement the policy.

Exhibit A	Draft Contract Language for 3rd party IT Services

Exhibit A - Draft Contract Language for 3rd party IT Services*

**This draft contract language is provided as strictly a guideline for AU faculty & staff. Alvernia University recognizes that not all 3rd party contracts will include the language suggested in this Exhibit A.*

[Provider] agrees to implement security controls to protect the confidentiality, integrity, and availability of the AU data and processes supported under this contract.

Definitions

Capitalized terms used herein shall have the meanings set forth in this Section.

"Authorized Employees" means Service Provider's employees who have a need to know or otherwise access Customer Information to enable Service Provider to perform its obligations under this Agreement.
"Authorized Persons" means (i) Authorized Employees; and (ii) Service Provider's contractors, agents, outsourcers, and auditors who have a need to know or otherwise access AU Information to enable Service Provider to perform its obligations under this Agreement, and who are bound in writing by confidentiality obligations sufficient to protect this Information in accordance with the terms and conditions of this Agreement.

"Security Breach" means any act or omission that materially compromises either the security, confidentiality or integrity of AU Information or the physical, technical, administrative or organizational safeguards put in place by Service Provider (or any Authorized Persons) that relate to the protection of the security, confidentiality or integrity of that Information.

Security and Accessibility-related Terms & Conditions

(a) Service Provider acknowledges and agrees that, in the course of its engagement by Customer, Service Provider may receive or have access to Customer Information. Service Provider shall comply with the terms and conditions set forth in this Agreement in its collection, receipt, transmission, storage, disposal, use and disclosure of such Customer Information and be responsible for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of Customer Information under its control or in its possession by all Authorized Persons. Service Provider shall be responsible for, and remain liable to, Customer for the actions and omissions of all Authorized Persons concerning the treatment of Customer Information as if they were Service Provider's own actions and omissions.
(b) In recognition of the foregoing, Service Provider agrees and covenants that it shall: (i) keep and maintain all Customer Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure; (ii) use and disclose Customer Information solely and exclusively for the purposes for which the Customer Information, or access to it, is provided pursuant to the terms and conditions of this Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Customer Information for Service Provider's own purposes or for the benefit of anyone other than Customer, in each case, without Customer's prior written consent; and (iii) not, directly or indirectly, disclose Customer Information to any person other than its
Authorized Persons, including any, subcontractors, agents, outsourcers or auditors (an "Unauthorized Third Party"), without express written consent from Customer unless and to the extent required by Government Authorities or as

otherwise, to the extent expressly required, by applicable law, in which case, Service Provider shall (i) use best efforts to notify Customer before such disclosure or as soon thereafter as reasonably possible]; (ii) be responsible for and remain liable to Customer for the actions and omissions of such Unauthorized Third Party concerning the treatment of such Customer Information as if they were Service Provider's own actions and omissions.

(c) Service Provider agrees to implement and maintain appropriate information technology security controls in the following areas, as outlined in **AU Policy 9.4000, IT Security for 3rd Party Partners and providers**; and **NIST Special Publication 800-171**, **Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations** (incorporated by reference).

d) If the Service Provider is hosting AU data on a multi-tenant system, these controls must include controls to prevent the unauthorized access of AU data to other tenants.

- i) Access Control
- ii) Awareness and Training
- iii) Audit and Accountability
- iv) Configuration Management
- v) Identification and Authentication
- vi) Incident Response
- vii) Maintenance
- viii) Media Protection
- ix) Personnel Security
- x) Physical Protection
- xi) Risk Assessment
- xii) Security Assessment
- xiii) System and Communications Protection
- xiv) System and Information Integrity

e) [required only if the service provider will be handling confidential or payment card data] The service provider must Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:

- Firewalls
- IDS/IPS
- Identity Management
- Anti-virus
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls (if used)

f) [required only if the service provider is providing a web-based interface to prospective or current students] The system provided must accessible to those with disabilities. Specifically, it must meet Web Content Accessibility Guidelines 2.0 (WCAG 2.0) Level AA published by the World Wide Web Consortium (W3C) and the Web Accessibility Initiative Accessible Rich Internet Applications Suite (WAI-ARIA) 1.0 guidelines.