Information Security Standard 15.1a

Supplier Relationship Security Standard

Initially Approved: April 19, 2017
Revised August 21, 2020 (as the Supplier Relationship Security Standard)
Administering Office: Office of the CIO

I. STANDARD STATEMENT

This standard operates under University Policy 117 Information Security.

The security of information processed, transmitted or stored by organizations contracted by WCU to provide those services needs to be insured. This means that WCU must put in place and manage contracts that protect the confidentiality, integrity and availability of information handled by suppliers of these services.

II. SCOPE AND APPLICATION OF THE STANDARD

This standard affects all WCU information technology systems that are supported by suppliers, whether the system or service provided is on-premise or not.

III. DEFINITIONS

a. "Suppliers" shall mean vendors, contractors or other third-parties that provide software or IT services to WCU through a contract or other agreement.
b. "Soft token" shall mean a software-based security token that generates a single-use login PIN.
c. "RFP" shall mean either a request for proposal or an invitation for bid.

IV. SUPPLIER RELATIONSHIP SECURITY STANDARD

a. IT Division Practices

i. Access Control

1. Supplier Accounts

a. Access must be granted to suppliers only when required for performing work and with the full knowledge and prior approval of the data steward or their designee for the pertinent data
b. Access must be granted on a temporary basis to

suppliers per University Policy 95, utilizing the Request Supplier Account form found in myWCU

c. Suppliers must request individual accounts for each user accessing WCU systems. Exceptions to the single user per supplier account must be approved by the CIO
d. Suppliers shall be fully accountable to WCU for any actions taken while performing work and shall abide by the data security requirements of the Confidentiality Agreement (part of the Access Request Form), in addition to the terms of the contract.

2. Multi-factor authentication

a. Suppliers needing access to systems that require multi-factor authentication must do so from an account tied to an individual using WCU's standard methods
b. When an exception to the single individual per supplier account is approved multi-factor authentication to the account must be accomplished by utilizing a soft token mechanism.

ii. Remote Access Monitoring

When required for regulatory compliance supplier access to on-premise systems must be monitored or logged. This may be done using active monitoring by staff or by session logging done with software.

iii. Service Data Security Monitoring

Per the WCU Data Handling Procedures, access must be re-certified and security controls must be audited periodically for RED and ORANGE data. Where this data is stored off-campus, a periodic audit of compliance with the data security requirements of the contract shall be coordinated by WCU IT.

b. Contract Requirements

i. IT contract requirements

Contracts that relate to services where WCU data is stored off-campus must utilize the standard WCU IT contract addendum, or contract language that sufficiently insures the security of the data. Also, a completed copy of the EDUCAUSE Higher Education Cloud

Vendor Assessment Tool must be provided by the supplier as part of the RFP process prior to signing a contract.

When purchasing software solutions, either hosted or on-premise, where WCU has not issued an RFP then the supplier must complete the WCU IT Solution Initial Assessment Tool. Responses to this tool must be analyzed and approved by WCU IT prior to signing a contract.

ii. HIPAA Business Associates

WCU mandates that all suppliers with access to WCU electronic protected health care information ("ePHI") follow the University's HIPAA Policy and related information security policies as a condition of the relationship.

WCU has developed standard language for business associate addenda to contracts. WCU staff must not negotiate new language without approval of WCU Legal Counsel.

If WCU knows of a pattern of activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation under the contract or inter-agency agreement, WCU must:

- Ensure that the business associate takes reasonable steps to cure the breach or end the violation, including working with and providing consultation to the business associate; or
- Terminate the contract, if such steps are unsuccessful; or
- If termination is not feasible, report the problem to the U.S. Department of Health and Human Services.

iii. PCI Service Providers

Payment Card Industry Data Security Standards (PCI) require that organizations that process, transmit or store payment card information on behalf of WCU are considered service providers and must agree to their role in fulfilling the requirements for PCI-compliance. If the contract with the service provider does not sufficiently address this then the service provider must sign WCU's PCI Service Provider Agreement Addendum.

V. REVIEW

This standard and the contract addendums mentioned herein will be

reviewed periodically and updated as necessary.

VI. REFERENCES

International Standards Organization (ISO/IEC 27002, 15.1 Information security in supplier relationships)

45 CFR Part 164, Subpart C, Security and Privacy

University Policy 117 Information Security

University Policy 95

WCU Data Handling Procedures

EDUCAUSE Higher Education Cloud Vendor Assessment Tool

WCU IT Solution Initial Assessment Tool

IT Contract Addendum

HIPAA Business Associate Contract

PCI Service Provider Agreement Addendum