West Texas A&M University™

The Division of Information Technology
University Information Security Standards

NIST CONTROL FAMILY
IDENTIFICATION AND AUTHENTICATION CONTROLS

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVIEW DATE
SA-4	**Acquisition Process**	**P1**	**07/23/2017**

I. STATEMENT

Overseeing the acquisition of information system products and services plays an important role in supporting the management of technology (e.g., hardware, software, and services) for the University. Establishing limits for security and access controls reduces the overall risk of liability, embarrassment, loss of revenue, loss of data, or loss of trust to the university and the community.

II. APPLICABILITY

This Control applies to all West Texas A&M University personnel who currently have, or will have, a vendor, third party or cloud computing service provider agreement or contract. The procedures in this control shall be applied to new contracts or agreements, renewal of existing contracts or agreements, the necessary review of existing contracts or agreements when security mandates change, and all amendments to existing contracts or agreements. Information resources contracts must include all terms required in this control.

III. IMPLEMENTATION

1. OWNER OF AN INFORMATION RESOURCE RESPONSIBILITIES

1.1 A risk assessment should be conducted prior to engaging any technology agreement or contract.

1.2 To assure compliance with this section, owners of information resources, or their designees, entering into a contract for services with a third party or cloud computing service provider must supply a written memo to the university's contract administration office and the chief information officer. At the time the contract is submitted for review, it must indicate that the third party or cloud computing service provider will have access to mission critical and/or confidential information.

1.3 The owner of the information resource, or designee, will coordinate review of formal modifications or contract amendments through the university contract administration office and the chief information officer if it is necessary to renew or modify a third party or cloud computing service provider contract or agreement with the university.

1.4 The departmental unit managing the procured service shall maintain accountability for the privacy and security of institutional data.

1.5 Access to mission critical and/or confidential information shall be granted only by explicit authorization of the owner of an information resource or designee and in coordination with the university's Chief Information Officer and Information Security Officer. Documentation of the access authorization shall be maintained by the owner of an information resource or designee.

1.6 Before cloud services contracts are signed, the Chief Information Officer and the Information Security Officer shall be notified that a cloud service is being considered so a review process can be initiated.

1.7 In all instances where institutional data is, or will be, stored outside of the university network, the Chief Information Officer and the Information Security Officer shall be notified.

1.9 The Chief Information Officer and the Information Security Officer shall be notified, shall be consulted before PII, PHI, or confidential institutional information is, or will be, manipulated in a cloud environment.

2. THIRD PARTY OR CLOUD COMPUTING SERVICE PROVIDER RESPONSIBILITIES

2.1 Third party or cloud computing service provider personnel are responsible for being familiar with all contract requirements which includes adhering to all applicable university Rules, SAPs, and Controls.

2.2 Contracts and agreements shall require third party personnel and cloud computing service provider personnel to report all incidents, suspected or confirmed, that affect institutional data directly to the university Information Security Officer or designee as soon as practically possible.

3. UNIVERSITY CONTRACT ADMINISTRATION

3.1 The university contract administration office is responsible for incorporating appropriate language into contracts related to information resources and information security.

4. CONTRACT STIPULATIONS

4.1 Owners of information resources shall ensure that third parties or cloud computing service providers who are granted access to mission critical and/or confidential information have contracts or agreements that specify the information in the following sections.

4.2 Required information that should appear in an IT contract:

4.2.1 The university information resources to which the third party or cloud computing service provider should have access will be stated how mission critical and/or confidential information is to be protected by the third party or cloud computing service provider.

4.2.3 Third parties and cloud computing service providers must follow industry best practices regarding change control processes and related procedures.

4.2.4 Acceptable methods for the return, destruction, or disposal of mission critical and/or confidential information in the third party's or cloud computing service provider's possession at the termination of the contract shall be explicitly stated.

4.2.5 Third parties or cloud computing service providers shall comply with terms of applicable non-disclosure agreements, which shall be stated.

4.2.6 Regular work hours and duties shall be defined in the contract.

4.3 Clauses that should appear in IT contracts with only minimal changes:

4.3.1 The use of university mission critical and/or confidential information and information resources are only for the purpose of the business agreement.

4.3.2 Any university information acquired by the third party or cloud computing service provider in the course of the contract or agreement cannot be used for the third party's or cloud computing service provider's own purposes or be divulged to others.

4.3.3 When practical, third parties and cloud service providers shall provide two factor authentication for user access to confidential or controlled information that is stored or is in motion across the internet.

4.3.4 The owners of the information resources or designees shall identify a university employee(s) as a local point of contact for the contract or agreement. The university point of contact will ensure that the third party or cloud computing service provider is aware of their obligation to understand and observe published university policies.

4.3.5 Each third party or cloud computing service provider shall provide the university point of contact with the name of a representative assigned as the key contact for the contract or agreement.

4.3.6 When third parties have an onsite presence at the university, a list of employees assigned to the contract shall be provided to the university point of contact.

4.3.7 Any onsite work outside of defined parameters must be approved in writing by the owner of the information resource or designee when third parties are on site at the university.

4.3.8 Information resources devices that utilize permanent memory storage must contain provisions to protect or destroy any restricted personal information, confidential information, mission critical information, intellectual property, or licensed software when the device is not directly under the control of West Texas A&M University.

4.3.9 Third parties and cloud computing service providers who are granted access to mission critical and/or confidential information resources shall comply with all federal, state, and university policies, rules, standards, practices and agreements including but not limited to FERPA, HIPAA, PCI, GLBA, GDPR, safety, privacy, security, auditing, software licensing, acceptable use, and nondisclosure requirements. Formal acknowledgement of this responsibility shall be provided to the owner of the information resource, or their designee, and incorporated into any applicable third party or cloud computing service provider contract.

4.3.10 All third parties and cloud computing services shall agree and understand that institutional data may be subject to e-discovery demands, Texas State auditing requirements, Texas State Public Information Act requirements, or university directed forensics investigations.

5. PRIVACY

5.1 Confidential information, including PHI and PII, may be managed by a cloud service only when there is a contract in place with the university.

6. RESEARCH COLLABORATORS

6.1 At the discretion of the Chief Information Officer or Information Security Officer, research collaboration related to information resources may not require a formal contract on an individual project basis. However, the research collaborator (i.e., university employee) is still responsible for following all other university Rules, SAPs, and Controls

7. QUESTIONS

7.1 Questions concerning information technology security shall be referred to the university's information security officer @ security@wtamu.edu.