System Acquisition Security Risk Survey for Service Providers

This survey was developed to gather information that is necessary to assess the potential security risks of adopting, acquiring, or integrating a new system or application into the UNT computing infrastructure. This survey also takes into account risks associated

General Information

Company Name

Representative Name

Representative Title

Representative Contact Information (telephone and e-mail)

Date of Response

System and Data Security

Where will the system, application, or service be housed?

Who operates and maintains the facility where the servers will be housed?

Who are the parties involved in providing this service? (cloud services, third party, etc.)

Can the system, application or service be accessed remotely?

Who can access the system, application or service?

What protections are in place to protect the data from unauthorized access?

What authentication is required for the system, application, or service?

What system or application security controls are in place to ensure th

What physical security controls are in place to ensure that the system

What is the emergency response capability of the entity who will manage the system?

Is a disaster recovery plan in place? How often is it tested?

Is there an information security policy in place that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the policy?

What environmental controls are in place to ensure that the system

Encryption

Confidential information and sensitive personal information must

How are confidential data encrypted in transit?

How are confidential data encrypted at rest?

If data are not encrypted, what steps are in place to mitigate the

Confidentiality of Personal Information

Is personal information - provided by the client - shared with third parties (other than your company or organization)?

What controls have been referenced within the contract or agreement for this service that ensure that personal information shared with third parties is appropriately protected by the third party?

What documented controls and procedures are in place that

Additional Required Information

Please submit the following in addition to this document:

1. Security plan for the application, service, infrastructure and data.

2. Business continuity or disaster recovery plan that is in place that ensures customer access to the service/information in the event of a loss or disruption of services.

3. Security plan implemented by third-parties (other than your company or organization) that will process, transmit, or manage data on behalf of your company or organization.

Service Provider Response	Texas Administrative Code Reference (Part 1, Title 10)	ISO Ref Num
University of Texas/ Texas Digital Library		
Ryan Steans		
Director of Operations		
512-495-4403 rsteans@austin.utexas.edu		
12/12/2014		
Amazon Web Service	202.73(a)	
Amazon Web Service	202.73(a)	
Amazon Web Service, DLT Solutions, TDL.org	202.75(2)(B)	
Yes	202.75(1)	11.7
Only staff with SSH key access	202.75(1)	
TDL provides all systems with	202.75(1)	
system: ssh key, application: shibboleth	202.75(3)(A)-(E)	11.2.1.a
Firewall, private ssh key management	202.74(A) and (B); 202.75(2) and (4)	
Amazon EC2 physical securities	202.73	
Hosted systems are managed and monitored to report outages. During working hours, this is monitored continually. After hours, monitoring is sporadic. Response of TDL staff is to alert member of outage/ issue immediately and provide continual, hourly updates.	202.74	
TDL has a disaster recovery plan and it has been tested with previous disasters, by successfully reinstating the service with no loss of data.	202.74	
It has not been communicated to constituents.	202.75(7)	5.1.1

Amazon EC2 environmental controls	202.73(c)
https	202.75(4)
postgresql hashes	202.75(4)
	202.75(4)
no	202.75(4)
we do not share with third parties unless the option is selected by the students submitting their thesis choose to share data.	202.75(4)
data. We also require managed user accounts	202.75(4)

ISO Ref Text

Mobile Computing And Teleworking

User Registration

Information Security Policy Document