Texas A&M University-San Antonio

29.01.99.O0.01 Information Resources - State Web Sites
Approved: June, 2012
Reviewed: January, 2015
Next Scheduled Review: January, 2019

Procedure Statement

This Procedure establishes the processes that Texas A&M University-San Antonio (A&M-San Antonio) will follow to comply with the privacy, linking, and indexing requirements for state Websites as stated in Texas Administrative Code (TAC), Title 1, Ch. 206, State Websites. The accessibility and translation portions of the requirements are covered in A&M-San Antonio Procedure 29.01.04.O0.01 *Accessibility of Electronic and Information Resources*.

Reason for Procedure

This Procedure is required by Texas A&M University System (System) Policy 29.01 *Information Resources*.

Official Procedure

1. PRIVACY

1.1 Privacy of information shall be provided to users of A&M-San Antonio information resources consistent with obligations of Federal and Texas State Law and/or secure operation of University information resources.

1.2 Electronic files created, sent, received, or stored on University owned, leased, administered, or otherwise under the custody and control of A&M-San Antonio are not private and may be accessed by authorized A&M-San Antonio information technology employees at any time without knowledge of the information resource owner or owner.

1.3 To manage systems and enforce security, A&M-San Antonio may log, review, and otherwise utilize any information stored on or passing through its information systems in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards. For these same purposes, A&M-San Antonio may also capture user activity such as telephone numbers dialed and Web sites visited. In the normal course of their duties, system administrators may examine user activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware.

1.4 In order to protect against hardware and software failures, backups of all data stored on University information resources may be made. System administrators have the right to examine the contents of these backups to gather sufficient information to diagnose and correct problems with system software, hardware, or performance. It is the user's responsibility to find out retention policies for any data of concern.

1.5 A wide variety of third parties have entrusted their information to A&M-San Antonio for business purposes, and all workers at A&M-San Antonio must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.

1.6 The organization head may designate certain individuals or functional areas that may monitor user activities and/or examine data solely to determine if unauthorized access to a system or data is occurring or has occurred. If files are examined, the file owner will be informed as soon as practical, subject to delay in the case of an on-going investigation.

1.7 To manage the efficient operation of information systems, appropriate security practices, and issues relating to inappropriate or illegal use of information resources, the University may log, review, and otherwise utilize any information stored on, or passing through, its information resource systems. All such actions shall be in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Security Standards, and other applicable rules and laws.

1.8 Files owned by individual users are to be considered as private, whether or not they are accessible by other users. The ability to read a file does not imply consent to read that file. Under no circumstances may a user alter a file that does not belong to him or her without prior consent of the file's owner. The ability to alter a file does not imply consent to alter that file.

1.9 If criminal activity is suspected, the University Police Department or other appropriate law enforcement agency must be notified. All further access to information on University information resources must be in accordance with directives from law enforcement agencies.

1.10 Information resource owners or custodians will provide access to information requested by auditors in the performance of their jobs. Notification to file owners will be as directed by the auditors.

1.11 Unless otherwise provided for, individuals whose relationship with the University is terminated (e.g. student graduates, employee takes new job; termination; visitors depart) are considered to cede ownership to the information resource custodian. Custodians should determine what information is to be retained and delete all other.

1.12 The University collects and processes many different types of information from third parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations (e.g., Gramm-Leach-Bliley Act, Texas Administrative Code 206).

1.13 Individuals who have special access to information because of their position have the absolute responsibility to not take advantage of that access. If information is inadvertently gained (e.g. seeing a copy of a test or homework) that could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the organizational unit head.

1.14 Users of A&M-San Antonio information resources shall call the Information Technology Helpdesk to report any compromise of security which could lead to divulging confidential information including, but not limited to, posting Social Security and credit card numbers to the Internet.

1.15 Users shall not attempt to access any University data or systems that they do not have authorization or explicit consent from the owner or appropriate University employee to access.

1.16 University Web sites available to the general public shall contain a Privacy Statement.

2. INDEXING AND LINKING

2.1 All TAMU homepages and key public entry points must include a link to the “Site Policies” and “Web Accessibility” pages.

2.2 All Web pages shall avoid vendor specific, “non-standard” extensions and shall comply with applicable internet standards. For example, use: IETF for internetworking technology or methodology (e.g., SSL); and W3C for markup/style sheet languages (HTML, XML, CSS, etc.).

2.3 All Web pages must implement the following:

2.3.1 Metadata, following the TRAIL Meta-tagging Standards (see http://www.tsl.state.tx.us/trail/about.html for more information). The descriptors of TRAIL Meta tags must describe the specific Web page or publication in which they are included. Use of a generic set of descriptors for every publication is not acceptable. The following Meta tags must be implemented:

2.3.1.1 DC.Subject.Keyword
2.3.1.2 DC.Description
2.3.1.3 DC.Subject

2.3.1.4 DC.Type
2.3.1.5 The HTML TITLE Tag

2.3.2 University campus homepages must contain

2.3.2.1 Links to the following State of Texas resources:
2.3.2.1.1 State of Texas homepage
2.3.2.1.2 Texas Homeland Security Website
2.3.2.1.3 Statewide Search Web site
2.3.2.1.4 State Link Policy or to a TAMU Link/Site Policy page

2.3.2.2 Individual links to the following or to the Site Policies page with links to the following:
2.3.2.2.1 Privacy and Security Policy
2.3.2.2.2 Accessibility Policy
2.3.2.2.3 Institution of higher education contact information
2.3.2.2.4 Description of policy/procedures related to the Open Records/Public Information Act
2.3.2.2.5 Compact with Texans

2.3.3 Key Public Entry Points must provide links to the following:

2.3.3.1 University campus homepage
2.3.3.2 Individual links to the following or to a Site Policies page containing links to the following:
2.3.3.2.1 University Contact Information
2.3.3.2.2 Accessibility Policy
2.3.3.2.3 Privacy and Security Policy

Related Statutes, Policies, Procedures, or Requirements

Texas Administrative Code, Title 1, Ch. 206, *State Websites*

System Policy 29.01 *Information Resources*

A&M-San Antonio Procedure 29.01.04.O0.01 *Accessibility of Electronic and Information Resources*

Definitions

Information Resource Owner – an entity responsible for:
- a business function; and,

- determining access controls to information resources supporting that business function.

Metadata - Data about data; index-type data used to identify, describe, locate, or preserve (other) data over time.

Contact Office

Finance and Administration, Information Technology Services (210) 784-4357 (HELP)

Appendix

Privacy & Security Statement

Purpose

Texas A&M University-San Antonio respects your privacy and is committed to ensuring that any personal or confidential information that is collected is kept accurate and secure from unauthorized access. The University's campus homepage, and any other campus Web site linking to this page does not collect personal information about visitors. We may, however, use third party analytics services that may use browser cookies to anonymously collect and track site usage information. This information is then analyzed as an aggregate, and no personally identifiable information is collected.

Scope

This Privacy and Security Statement applies to the A&M-San Antonio campus homepage - www.tamusa.tamus.edu and any site explicitly linking to it. Since the A&M-San Antonio Web community consists of many Websites, other Web sites may adopt different privacy and security statements as their specific needs require. The A&M-San Antonio homepage, as well as other sites across campus, contain links to various external Web sites. The University is not responsible for the privacy and security practices or the content of external Web sites linked to.

Information Gathered by A&M-San Antonio

Personal information that you provide via email or through other online means will be used only for purposes necessary to serve your needs, such as responding to an inquiry or other request for information. This may involve redirecting your inquiry or comment to another person or department better suited to meeting your needs. Our site does use server logs to collect information concerning your internet connection and general information about your visit to our Web site. This information may be used to analyze trends; to create summary statistics for the purpose of determining technical design specifications; and to identify system performance or problem areas. This means we sometimes acquire, record, and analyze portions of the data that is entered into, stored on, and/or transmitted through this site by you. This information is only released – when legally required – to help law enforcement investigations, legal proceedings or internal investigations of violations of System Policies & Regulations or A&M-San Antonio Rules & Procedures. These groups would use the information to track the electronic interactions back to the source computer(s) or account(s).

Cookies

A cookie file contains unique information that a Web site can use to track such things as passwords, pages you have visited, the date you last looked at a specific page, and to identify your session at a particular website. We do not use cookies to track or collect any information that could personally identify individual visitors.

Server Log Information

The following information may be collected from server logs utilizing the services of Google Analytics and/or Rackspace analytics for analysis. Note that other servers across campus might collect different data elements.

- User/client hostname - The hostname (or IP address if DNS is disabled) of the user/client requesting access
- HTTP header, "user agent" - The user-agent information includes the type of browser, its version, and the operating system it is running on
- HTTP header, "referrer" - The referrer specifies the page from which the client accessed the current page
- System date - The date and time of the user/client request
- Full request - The exact request the user/client made
- Status - The status code the server returned to the user/client
- Content length - The content length, in bytes, of the document sent to the user/client
- Method - The request method used
- Universal Resource Identifier (URI) - The location of a resource on the server
- Query string of the URI - Anything after the question mark in a URI
- Protocol - The transport protocol and version used

Some Web pages at Texas A&M University-San Antonio may collect personal information about visitors and use that information for purposes other than those stated above.

Access to Information

Except for education records governed by FERPA, all information collected from this Website, including the summary server log information, emails sent to the Web site, and information collected from Web-based forms, may be subject to the Texas Public Information Act. This means that while A&M-San Antonio does not actively share information, in some cases may be compelled by law to release information gathered from its Web servers. The Texas Public Information Act, with a few exceptions, gives you the right to be informed about the information that this Web site collects about you. It also gives you the right to request a copy of that information, and to have the University correct any of that information that is wrong. You may request to receive and review any of that information, or request corrections to it, by contacting the Public Information Officer in the University Communications Department at (210) 784-1101.

Security

Extensive security measures consistent with the Texas Administrative Code "Information Security Standards" and A&M-San Antonio Rules and Procedures have been employed to protect against unauthorized access, disclosure, modification, or destruction of information under our control, as well as the loss, misuse, or alteration of this website and/or associated electronic information resources. The information resources that support this site undergo an annual information security risk assessment via the Information Security Awareness Assessment and Compliance (ISAAC) system. The ISAAC system is used to assess the security posture of information systems and measure compliance with information security standards.

Questions

If you have any questions about the practices of this site or your use of this website, please contact the Multimedia and Web Coordinator at:

Texas A&M University-San Antonio
University Communications
Attention: Multimedia and Web Coordinator
One University Way
San Antonio, Texas
78224. (210) 784-1102