29.01.99.C1.01 IT Acceptable Use and Privacy

Approved June 1, 2016
Revised June 1, 2016
Next Scheduled Review June 1, 2018

Procedure Statement

This Procedure defines primary rights and responsibilities for all users of information and information resources that belong to, or under the control of Texas A&M University – Corpus Christi ("University"). More detailed explanations of these rights and responsibilities may be found in the IT Standard "IT Standards for All Users."

Reason for Procedure

This Procedure applies to all information and information resources owned or under the control of the University, and to all people ("users") who access those resources and information. The audience for this Procedure is all users.

The purpose of this Procedure is to educate users as to their rights and responsibilities as users.

Users may assume other information-technology roles (e.g., Owner, Custodian) in addition to user. With those other roles come other rights and responsibilities which are detailed in separate documentation called IT Standards for Owners and Custodians.

The purpose of the implementation of this University Procedure is to provide a set of measures that will mitigate information-security risks.

Procedures and Responsibilities

1. ACCEPTABLE USE

1.1. GENERAL

1.1.1. As an institution of higher learning, the University encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. The University recognizes the importance of information technology to students, faculty and staff in scholarly pursuits, professional development, service activities, personal development and every day work and class-related activities. In particular, access to networked electronic

information (e.g., the Internet) supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines.

1.1.2. As such, the University makes available information resources (e.g., facilities, networks, hardware, software) and information for use by members of the community. Such use must be acceptable, i.e., such use must comply with all relevant law and policy, including federal law (e.g., FERPA), state law (e.g., TAC 202), Texas A&M University System Policies and Regulations, University Rules and Procedures, relevant IT Standards, and the University's Student Code of Conduct.

1.1.3. This section addresses, in general terms, the University's philosophy about computing use and provides an overview of some of the more important law and policy regarding such use. However, it is the responsibility of all users to ensure that their use complies with all relevant law and policy. In particular, all users should review "IT Standards for All Users" for a more detailed explanation of IT acceptable use.

1.1.4. Censorship is not compatible with the goals of the University. The University should not limit access to any information due to its content when it meets the standard of legality and is compatible with authorized use. Forms of expression that are not protected by the First Amendment, and therefore may be subject to censorship by the University include obscene material, child pornography, or other violations of the law. Also, the University may block access to content that jeopardizes the security of University information-resources and University information, e.g. websites containing malware.

1.2. ACCEPTABLE USE PROCEDURES

1.2.1. Only Authorized Use. A user shall not use or attempt to use a University information-resource or University information unless and until the Owner of the information resource or information has authorized such use.

1.2.1.1. A user shall use a University information-resource or University information only in the manner authorized by the Owner. For example, if an Owner has authorized a user only to view certain information, then the user is not permitted to edit that information even if the user has the technical ability to do so.

1.2.2. Only Legitimate Institutional Use and Permissible Incidental Use. All use must be either 1) legitimate institutional use or 2) permissible incidental use. Legitimate institutional use is use that 1) is reasonably related to the user's official duties with respect to the University (e.g., teaching, research, administration), and 2) furthers

the University's mission. Permissible incidental use is defined in Texas A&M System Policy 33.04.

1.2.3. Only Lawful Use. All use must comply with all relevant law and policy, including federal law, state law, Texas A&M System Policies and Regulations, and University Rules, Procedures and Standards.

1.2.4. Protect Confidential and Controlled Information. Users must protect confidential and controlled information from unauthorized disclosure, modification, or deletion. See, e.g., Family Educational Rights and Privacy Act (FERPA), Texas Public Information Act (TPIA), and the Payment Card Industry Data Security Standard (PCI-DSS).

1.2.5. No indecent or obscene material. Users shall not use University information resources to intentionally access, create, store or transmit material which University may deem to be indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the University official processes for dealing with academic ethical issues).

1.2.6. Authenticators (e.g., passwords). Users shall neither share their passwords nor accept or use the password of another.

1.2.7. No Private Commercial or Organized Political Use. With the exception of the limited purposes described in System Regulation 33.04.01, users shall not be paid, or otherwise profit, from the use of any University information resources or from any output produced from such resources. Users shall not use University information resources to promote non-University-related commercial activity or to conduct organized political activity that is inconsistent with the University's tax-exempt status.

1.2.8. Respect Copyright. Intellectual property laws (e.g., copyright) apply to the electronic environment and users shall respect such laws. Users should assume that information (e.g., documents, messages, software) stored on or communicated by University information resources are subject to copyright unless specifically stated otherwise. Users shall not make unauthorized copies of copyrighted software or other copyrighted materials such as music, films, and textbooks. The University complies with all legal requests for information and will not hesitate to report a user's use in response to a lawful request.

1.2.9. Hardware and Software. Users shall not 1) use or install unauthorized software or hardware, or 2) make unauthorized changes to University hardware and software. Please see "IT Standards for All Users" for a more detailed explanation of authorized and unauthorized software, hardware, and changes.

1.2.10. Only Ethical Use. All use of University information resources and University information must be ethical. (See System Policy 07.01, Ethics).

1.2.11. Other Impermissible Use. Users shall not use University information resources or University information to purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of University information resources; deprive an authorized user access to a University resource; obtain extra resources beyond those allocated; circumvent University information security measures. Users shall not otherwise engage in acts against the aims and purposes of the University as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

1.2.12. Physical Security. Users shall secure unattended portable devices. Users working on publicly-accessible computers shall logout or invoke a password-protected screensaver when leaving the computer.

1.2.13. Security Incident Reporting. Users shall report to the IT Helpdesk any weaknesses in the security of the University's information resources, or any incidents of possible misuse or violation of this or any other policy related to the security of the University's information resources.

2. IT PRIVACY

2.1. GENERAL

2.1.1. Privacy policies are mechanisms used to establish the responsibilities and limits for system administrators and users in providing privacy in University information resources.

2.1.2. Users of University information resources have a basic right of privacy in 1) the files they own which are stored or communicated by University information resources, and 2) the activities they perform using University information resources.

2.1.3. However, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.

2.1.4. In particular, the University has the right to examine all information stored on or passing through University information resources, and to monitor the activities of any user on University information resources so as to, e.g., ensure business continuity, ensure compliance with law and policy, or conduct authorized investigations.

2.2. PRIVACY PROCEDURES

2.2.1. A file may not be accessed, copied, or modified without prior authorization from the file Owner. This general right to privacy is subject to the following exceptions and limitations:

2.2.1.1. The file Owner's right to privacy in their files may be limited by other laws and policy. For example, the Texas Public Information Act may require the disclosure of certain data under certain conditions.

2.2.1.2. A person in the file Owner's chain of command (i.e., the file Owner's supervisor, that supervisor's supervisor, etc.) may access or copy any of the file Owner's files as long as that person has the authorization of the appropriate Dean or Vice President, i.e., the Dean or Vice President in the Owner's chain of command.

2.2.1.3. The IRM, his or her designees, and resource Custodians may log, monitor, copy, and examine any information passing through or stored on any University information resource for which they are responsible for reasons including, but not limited to:

2.2.1.3.1. Ensuring compliance with applicable law and policy;

2.2.1.3.2. Ensuring business continuity (e.g., making backups);

2.2.1.3.3. Monitoring network performance and maintenance activities, or;

2.2.1.3.4. Responding to authorized requests for information from, e.g., auditors or investigators.

2.2.1.4. In 2.2.1.2 and 2.2.1.3, the file Owner's authorization still should be sought before altering a file, except, e.g., where it would interfere with an authorized investigation, or in case of an emergency.

2.2.1.5. In response to lawful requests, the IRM may provide to authorized entities (e.g., law enforcement, auditors) access to information transmitted through and stored on University information resources after the notification and written approval of the Executive Vice President of Finance & Administration. Exceptions to this procedure may occur in instances related to federal and state laws.

2.2.2. A user's activities on or with a University information resource may not be tracked or recorded without first obtaining authorization from the user. This right of privacy in activities is subject to the following exceptions:

2.2.2.1. The IRM, his or her designees, and resource Custodians may, without any notification to a user, monitor some or all of the user's activities on relevant information resources for University- business-related purposes, including but not limited to those enumerated in 2.2.1.3. Examples of such monitoring include logging the phone numbers dialed by a user from their desk phone, or recording the web sites a user visited using a University workstation.

2.2.2.2. The University may perform video and audio surveillance as defined in other policy.

2.2.3. Individuals who have special access to information because of their position have the absolute responsibility not to take advantage of that access.

2.2.3.1. Such individuals should access only that information that is relevant to the particular task, and only so much of that information as is necessary to achieve the task

2.2.3.2. If, however, in the course of performing the task such individuals find unrelated evidence of impermissible use or other wrongdoing, those individuals are obligated to report an incident.

2.2.3.3. If an individual inadvertently accesses information (e.g., seeing a copy of a test or homework) that could provide personal benefit, such individual has the responsibility to notify 1) the file Owner, 2) their own supervisor, and 3) the file Owner's supervisor.

2.2.4. Unless otherwise provided for, individuals whose relationship with the University is terminated (e.g., student graduates; employee takes new job; visitors depart) are considered to cede ownership of, and hence the right to privacy in, all their files to the information resource Custodian. The University should determine what information is to be retained and delete all other.

2.2.5. Custodians of web sites available to the general public from University information resources shall abide by and ensure that those web sites contain a link to the University's privacy statement located at http://www.tamucc.edu/privacy.htm.

3. CONSEQUENCES FOR VIOLATIONS

3.1. All users, including staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors, are required to adhere to this University procedure, and may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and University policies.

3.2. Individuals found in violation of this University Procedure are subject to loss of access privileges to University information resources (e.g. servers, workstations, email, etc.) In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Related Statutes, Policies or Requirements

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M University-Corpus Christi IT Standard "IT Standards for All Users"
- Texas A&M System Policy
    - 01.03 Appointing Power and Terms and Conditions of Employment
    - 07.01 Ethics Policy, TAMUS Employees
    - 32.02 Discipline and Dismissal of Employees
    - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
    - 33 Employment, Standards of Conduct
    - 33.04.01 Use of System Resources for External Employment
- Texas A&M University-Corpus Christi Rule
    - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
    - 13.02.99.C1 Student Disciplinary Proceedings
    - 29.01.99.C1 Security of Electronic Information Resources

Definitions

Authenticators – account names and passwords, security access cards, tokens, and keys associated with mechanisms that permit access to information resources.
Confidential information – Information that is exempted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws. Most student records are confidential records. Examples of "Confidential" data include but are not limited to: social security numbers, grades, credit card numbers, and personal health records.

Contractor – any company, and its employees, not affiliated with Texas A&M University-Corpus Christi, which provides a service to the University.

Controlled information – Information that is not generally created for or made available for public consumption but that may be subject to public disclosure through the Texas Public Information Act or similar laws. Examples of controlled information include but are not limited to: operational information; personnel records; information security procedures; research; internal communications.

Custodian (of information or an information resource) – A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.

Information resources – The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Resources Manager ("IRM") - An institutional role defined by Texas Government Code, Section 2054.071 et seq. Appointed by the University President, the IRM has management authority over all University information resources.

Information Security Officer ("ISO") – University employee designated by the President to be responsible for all University information-security.

Malware – Software that is designed to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user's information systems, e.g. viruses, spyware.

Owner (of information or an information resource) – Person or entity authorized to decide which users may access the information resource and how. Not necessarily the owner in the sense of property.

Public information – Public information includes all information made available to the public through posting to public websites, distribution through email, or social media, print publications or other media. This classification also includes information for which public disclosure is intended or required.

Texas Administrative Code 202 ("TAC 202") – information security standards for information resources purchased by agencies and institutions of higher education in the State of Texas.

User – An individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

Vendor – see Contractor.

Contact Office

Office of Information Security, (361) 825-2124.