



The University Of

T A M P A

Information Security Data Classification and Protection Policy

Version: 2.0

Effective Date: 3/29/2016

Policy Summary:

University information will be categorized according to the levels of risk and harm that can result from disclosure or unauthorized use. Appropriate and relevant levels of access to University information will be provisioned and removed in accordance with university policies, procedures, and guidelines. Anyone handling University sensitive or confidential information is responsible for safeguarding this information from inadvertent or unintentional disclosure to unauthorized persons. Requirements regarding protection of regulated information (ex. FERPA, PCI, HIPAA) should be adhered to as outlined in the external compliance agency’s documented requirements and laws.

Questions about this policy should be directed to the UT Chief Information Officer at tclark@ut.edu or (813) 257-7522.

Applicability/Eligibility:

This policy applies to any individual, organization, group, entity, or third-party using University of Tampa computing or communications resources for information handling purposes. It encompasses but is not limited to all University wired and wireless networks, academic and administrative systems, e-mail, third party hosted websites, University websites and social media, faxed messages; University and personal computers, cellphones, and other mobile devices.

Exceptions:

None

Policy Administration:

Mandating Authority: Federal Law State Law or Regulation
(Check all that apply) University President Accrediting Body
 Other: (specify)

Responsible Office/Dept/Committee(s):

Name	Campus Address	Phone Number
Information Technology &	East Walker Hall Rm 133	813-257-7522

Security		
----------	--	--

Responsible Executive(s):

Name	Title	Phone Number
Tammy L. Clark	Chief Information Officer	813-257-7522

Policy Management:

Policy History:

Date	Version	Reason for Change
4/2/15	1.0	Initial policy draft
3/10/15	2.0	Incorporate organizational changes and enhancements to promote increased data protection

Policy Approvals and Reviews:

Date	Organizational Group
3/29/16	President
3/29/16	Senior Staff

Web Links:

Policy Link: [Information Classification and Protection Policy](#)

Associated Links:

[Third Party Service Provider Information Security Reviews](#)
[Acceptable Use Policy](#)

Full Policy Text:

University Data Classifications:

All university information data elements exist in one of three categories: **Confidential, Sensitive, or Public.**

- 1. Confidential Information.** Data for which the highest levels of restriction should apply due to the risk and harm that may result from disclosure or inappropriate use.

Examples of Confidential Data: Social Security Numbers, Credit Card Information, Electronic Protected Health Information (ePHI), Electronic Medical Records, Electronic Counseling records, Transcripts with Social Security Number.

- 2. Sensitive Information.** Data for which users must obtain specific authorization to access since the data's unauthorized disclosure, alteration, or destruction may cause perceivable damage to the institution and/or individuals affiliated with The University of Tampa.

Examples of Sensitive Information: Date of Birth, Purchasing Information, Students of Concern Reports, Campus Safety Incident Reports, Academic Grades, Transcripts without Social Security Number, University email.

3. Public Information. No access restrictions. Available to the general public.

University information that has been classified as **confidential** must have an identified **Data Owner**. **Data Owners** have primary responsibility for the privacy and security of the University data under his/her responsibility. **All** data users, not just **Data Owners**, Information Technology & Security staff, are responsible for the security and privacy of the information they access, transmit, and store.

Data Owners are responsible for ensuring that an approved process is followed or a security review has been successfully completed by the **Office of Information Security**, prior to granting access to confidential information.

Data Owners collaborate with the **Office of Information Security** by sponsoring policies, standards and/or guidelines that assist with meeting compliance requirements for regulated information. Examples: Payment Card Industry data (PCI) and Electronic Protected Health Information (ePHI).

Social Security Numbers. The University is required to collect SSNs from students, staff and faculty for legitimate business and reporting purposes. SSNs are classified as **confidential** and the University does not request, collect, store or otherwise utilize Social Security Numbers except when required. A social security number shall never be used as the primary identifier for a student, staff or faculty member in any University database system. University staff and faculty must ensure they do not submit images or documents containing visible Social Security Numbers, birth dates, or credit card numbers to systems that are not encrypted. The only exceptions to this policy are the university's authorized document imaging/storage system and the Student Information System.

Use of Encryption to Protect Confidential Information. Information Technology & Security will assist **Data Owners**, Information Technology departments, and anyone at the University handling confidential information in protecting this information through the use of encryption (conversion of data into a form that scrambles it so it cannot be understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood).

Use of Security Measures to Protect Information in Transit or Exchanged With External Parties. When sensitive or confidential information is transmitted and exchanged with external parties, the use of encryption and secure file transfer is necessary to protect this information from being intercepted by unauthorized persons. Email (unless encrypted), FTP, and electronic faxing programs that send the information over the internet are insecure methods of information exchange and users should not rely on these methods in conducting information exchanges. The Office of Information Security can assist campus departments with determining safe information exchange methods to use.

De-Identification to Protect Sensitive Information in Emails or other Communications. All campus departments are encouraged to use the Student ID in lieu of other description information in email, help desk tickets, or communications that are sensitive in nature. A student's name and ID are also appropriate if necessary. However, all care should be taken not to list full date of birth, name, address, and other contact information together, as this can

be used for nefarious purposes if accessed by unauthorized persons. Also, emails can be misdirected, so this inherently insecure medium must be used with discretion. Screen shots saved as images used for the purpose of creating help desk tickets must have confidential or sensitive information redacted.

Security Reviews. *Information Security* will perform security reviews of information handling processes upon request. Contact the ITS Helpdesk to request a security review.

Acceptable Use Policy. Compliance with the Acceptable Use Policy will also assist in ensuring sensitive and confidential information is adequately protected.

Assistance with Data Classifications: Any questions about classifying data types can be directed to infosec@ut.edu or 813-257-3950 and *Information Security* will be happy to assist.

Additional Information and Resources: [Information Security Guidelines for Data Owners](#)