THE UNIVERSITY OF TAMPA

OFFICE OF INFORMATION SECURITY

# Information Security Guidelines for Data Owners

***Contact The CISO, Office of Information Security to Discuss Information Security Policies and Guidelines:***

*Tammy Loper, Chief Information Security Officer (CISO), tloper@ut.edu, Ext.7522*

***Why is Classifying and Protecting Access to Specific Types of Information Important?***

*Staff, faculty, and students expect that their information will be properly protected and personal privacy preserved—and rightfully so. As public stewards, our institution has legal, contractual, and moral obligations to protect the institution's information resources and the confidential data of students, staff and faculty. Beyond this, the stakes for failing to protect data are high. A single undetected cyber-attack against an institution can lead to data exposures/breaches, and today most of these attacks are the result of employees and contractors succumbing to a phishing attack or a byproduct of 'loose' information and system access controls managed by the IT organization.*

***Why is Your Role as a Data Owner Important?***

*Your role has important information security and compliance responsibilities that must be understood and executed appropriately to safeguard information including:*

- *Collaborating with IT and Information Security to ensure a documented approval process is followed*
- *Coordination with Information Security to ensure confidential information is adequately protected*
- *Conducting periodic access reviews to ensure that individuals remain authorized to access information provided*

***A Data Owner's Eight Step Information Security Plan***

***Step 1: Get to Know Your Data – Inventory Your Department's Information Resources***

*Multiple security incidents at institutions of Higher Education have occurred involving exposure of information contained in data files that the data owner did not know existed. As you maintain an inventory of data for which your area is responsible, do not forget backups, test files, contracts and service level agreements. Also destroy data that is no longer needed.*

***Step 2: Get Assistance from The Office of Information Security***

*Make an appointment to meet with the CISO for an initial discussion about your area's information security needs.*

***Step 3: Classify Your Data***

*You need to know what data (type and quantity) your area is responsible for, where it is located and who has custody of it. At minimum, identify data this Confidential as defined by federal and state rules and other constitutional, statutory, judicial, and legal agreements/requirements.*

***Step 4: Establish Data Access Policies***

*Carefully consider who (which groups or roles) are authorized to view data and who is to be authorized to add, change, or delete data, and under what conditions. Define who, if anyone, is allowed to copy data for use on other computers and what uses are to be permitted.*

***Step 5: Specify Controls and Identify/Select Custodians***

*Determine which controls are provided by the Office of Information Security or the IT organization, as well as departmental employees. Determine if you are outsourcing custodianship to third parties that are hosting it for you—if so, you will need to work with the CISO as outlined in the* ***Third Party Service Provider Information Security Reviews policy****, to ensure necessary controls are in place.*

***Step 6: Establish a Culture of Information Security Awareness/Protection in Your Area***

*Many tasks can be delegated, but this cannot. As a university administrator/executive, you have tremendous influence over the attitudes and behaviors of your employees. Employees will tend to value and take their responsibilities in regards to data protection seriously if you require them to do so. In collaboration with the CISO, you are the messenger!*

***Step 7: Collaborate with The Office of Information Security in Performing Periodic Risk Assessments of your Area's Business Processes and Information Handling Practices***

*A risk assessment will continue to assist you in determining where gaps lie in information protection, whether through your area's business processes, information handling practices, or through the third parties that you work with. The need to review these aspects is ongoing, to ensure that information is not vulnerable or exposed to unauthorized parties.*

***Step 8:  Confirm that Controls Remain in Place***

*It is essential to collaborate with The Office of Information Security to ensure that approval processes and controls agreed upon remain in effect over time and are re-assessed when major changes occur that affects information resources.  Vigilance goes a long way!*

***How Can The Office of Information Security Assist You as a Data Owner?***

- *Meet with you to gain a general understanding of your business objectives and goals; challenges and needs; as well as what data falls under your area*
- *Use this understanding to advise you about data protection measures and controls*
- *Discuss and recommend information security services that you can request to assist you*
- *Discuss information security policies and assist you in classifying your data*
- *Assess the risk of making changes to existing services and solutions, switching vendors, and/or making changes in how you handle information.*