Data Security Framework (DSF)

Overview

The DSF will facilitate classification and protection of University data and systems based on associated SCORF risks (strategic, compliance, operational, reputation or financial risk) to the institution. Understanding the risk levels of different types of data is required for prioritizing investments in cybersecurity and ensuring equitable protection of data and systems. Following are key artifacts included in the DSF:

Policy - Information Asset Classification and Management Policy (IACMP). The current Data Classification Policy is being expanded to become the IACMP. The IACMP expands the classification criteria from focusing on data confidentiality (sensitivity) to also include data integrity and availability. This provides better alignment with university needs and industry best practices to protect data confidentiality, integrity and availability (CIA). The IACMP also includes classification of devices that process, store or transmit data. It simplifies the current classification policy by reducing the number of levels from 4 to 3 – "Public, Internal, Sensitive-Regulated, Sensitive-Unregulated" to "Low Risk (green), Moderate Risk (amber), and High Risk (red). Finally, the policy expands the responsibilities of data stewards accountable for ensuring security of university data and compliance with legal requirements. The redlined version of the policy is attached.

Standard – Data Security Classification Table. This table will be published online. It provides a listing of the most common data types, descriptions, examples of data elements, associated classifications, and responsible data stewards and custodians. See sample Data Security Classification Table snippet below.

Standard – Minimum Security Controls for Protecting Data and Systems by Classifications. These standards are currently being developed by the Information Security Office in collaboration with university IT staff, data stewards and custodians. They will provide administrative and technical requirements for protecting university data and systems wherever they reside. See sample standard below.

Process

The updated policy is currently under review by the Information Security Office in collaboration with data stewards and custodians across campus. It will be submitted for approval by the PAC during the May 1st session. The approved policy will be published along with the standards mentioned above, then a major training effort will be undertaken as part of the implementation of this policy. Finally, about 18 months after the policy is implemented, the Information Security Office in collaboration with the data stewards will develop and implement a formal program for monitoring compliance with the policy and associated standards.