**Perspectives in Information Security Data Owners**

**Office of Information Security Compliance**

* CISO contact information
* Staff contact information

**Office of Information Security Mission**

The Office of Information Security Compliance provides guidance and support to the institution's academic and health campuses in their efforts to establish and maintain information security programs that:

* Effectively reduce risk and secure the information assets under its stewardship against unauthorized use, disclosure, modification, damage, or loss
* Are documented and verifiable
* Meet regulatory compliance requirements

**Why Is Information Security Important?**

Students, employees, patients, granting authorities such as the National Science Foundation and the National Institutes of Health, and others who provide information to institutions of higher education or fund research expect that information will be properly protected and personal privacy preserved—and rightfully so. The institution, as a steward of public information, has legal, contractual, and moral obligations to protect its information resources and the confidential data of the employees, students, and patients it serves. Beyond this, the stakes for failing to secure data are high. A single successful cyberattack against an institution can lead to one or more of the following:

* Compromise of student, patient, or employee privacy
* Violations of the FERPA, HIPAA, or other federal or state regulations and increased regulatory oversight
* Disruption of patient care, instructional services, and administrative functions
* Loss of reputation for the institution
* Financial loss to the institution resulting from payments of mandated notifications or for providing credit-monitoring services to individuals whose personal data has been exposed, as well as payment of any regulatory fines
* Loss of good will and potential loss of donations and grants
* Loss or corruption of research data

**Why Is Your Role as Data Owner Important?**

Your role has important information security responsibilities that must be understood and executed to properly safeguard institutional information resources including:

* Approving access to information resources and periodically reviewing access lists
* Coordinating with your institution's information security officer (ISO) data security control requirements
* Conveying data security control requirements to custodians

But, most importantly, identifying, recommending, and documenting acceptable risk levels for information resources under your authority.

**A Data Owner's 8-Step Information Security Plan**

**Step 1: Get to Know Your Data—Inventory Your Information Resources Assets**

Multiple security incidents at institutions 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 you are responsible, do not forget backups, test files, contracts, and service level agreements. Also, destroy data that is no longer of use to the institution in accordance with institutional records retention schedules.

**Step 2: Meet with Your Information Security Officer**

Make an appointment to meet with your institution's ISO or a member of the ISO staff 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) is under your responsibility, where it is located, and under whose custody it is. At minimum, identify data that is confidential as defined by federal and state rules and other constitutional, statutory, judicial, and legal agreement requirements.

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

Carefully consider who (or which groups or roles) is to be 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 ISO or the central IT organization, which are to be provided by departmental employees, and which, if any, are to be outsourced. Make sure that all desired protections have been assigned.

**Step 6: Establish Information Security as a Value within Your Unit**

*Many tasks can be delegated, but this one cannot.* As administrative leader of your department, research project, or other institution unit, you have tremendous sway over the attitudes and behavior of others. Employees will tend to value and take information security seriously to the extent that you are perceived to do so. You are the message!

**Step 7: Perform Periodic Risk Assessments of Your High-Risk Resources**

A risk assessment will assist you in determining where to place protections and allocate security resources. It is a mistake to underprotect your resources, but it is also costly and ineffective to overprotect them. Use results from your risk assessment as another source for determining which security controls to implement.

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

It is essential that you periodically confirm that the controls you have specified and delegated to custodians remain in effect over time. Custodians are people too, and they can make errors. Verification is in your best interest, and in the best interest of the custodian. Finally, do not assume, simply on reputation, that a custodian has all essential controls in place. It is important to be vigilant and confirm controls.

**What Does the Office of Information Security Do to Assist You as a Data Owner?**

* Meet with you to gain a general understanding of your functional area including its mission and business functions and the data for which you are responsible.
* Use this understanding to advise you about protective measures appropriate for your area.
* Discuss and recommend general security services that the institution may provide centrally. You do not want to spend time and money acquiring services already available through services within the institution.
* Discuss data-classification policy and/or standards and assist you in the appropriate classification of your data.
* Discuss and recommend appropriate controls for your circumstances, business function, and type of data under your responsibility.
* Discuss your institution's risk assessment process and ensure that your area is included in future assessments.
* Assess the risk of development or purchase of new IT applications and services.