Information Owner's Guide to Data Protection

- Lessons Learned and Best Practices -

Information Owner's Guide to Data Protection

- Lessons Learned and Best Practices -

Audience and Purpose

The purpose of this document is to provide University administrators and others who serve in an "Information Owner" role with guidance needed to protect the information resources for which they are responsible. It is assumed that the reader is an Information Owner, therefore guidance is stated in the second person; it speaks to "you". Emphasis is on protection of "data" because experience indicates that the vast majority of information security attacks and breaches target an institution's data. This fact is reflected in the increase in federal and state regulations concerning data security and privacy enacted over the past few years.

Guidance provided herein is based on security incidents that have occurred within University of Texas System institutions, other universities, and other government agencies, lessons learned from these incidents, and best practices that should be used to prevent security breaches. Here you will find practical guidance designed specifically for individuals who are responsible for running University programs, departments, research operations, or other functions.

Throughout this guide, you will find "Lessons Learned." These are lessons relevant to the Information Owner role based on observations of incidents, their causes, and underlying contributing factors. The first of these relates to the need for Information Owner training.

> **Lesson Learned:** Some information security incidents are attributable, in part, to lack of understanding and execution of Information Owner responsibilities. Information Owners need specialized training and guidance regarding their unique information security responsibilities. This guide is one resource for providing guidance.

The "Information Owner" Role: The role of Information Owner is defined and assigned important information security responsibilities by Texas law. In practical terms, an Information Owner is usually the lead administrator of a University department, program, unit, or business function. Titles may vary considerably. Be it dean, chairman, director, principal investigator, manager, coordinator, etc. the person filling an Information Owner role has important information security responsibilities that must be understood and executed upon to properly safeguard University information assets. University policy refers to the role simply as "Owner". Within this guide, the terms "Information Owner, "Data Owner", and "Owner" have the same meaning and are used interchangeably. Your institution may have an established policy that formally identifies Information Owners. Check with your Information Security Officer.

Texas Administrative Code, Title 1, Part 10, §202.75 defines the "Information Owner" as, "A person with statutory or operational authority for specified information (e.g., supporting a specific business function) and responsibility for establishing the controls for its generation, collection, processing, access, dissemination, and disposal. The Information Owner may also be responsible for other information resources including personnel, equipment, and information technology that support the Information Owner's business function"

The *U. T. System Information Resources Use and Security Policy (UTS-165)* defines "Owner" as: "The manager or agent responsible for the business function that is supported by the information resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security and authorizing access to the information resource. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared."

Note that "shared ownership", though permitted by policy, increases risk. If you are in a shared ownership situation, confer with the other Owners and put in writing who the responsible party will be for the various Owner responsibilities.

Lesson Learned: When responsibilities are shared, it raises the risk that security tasks will fail to be performed because people assume tasks are being performed by another of the responsible parties. This is a common contributor to information security incidents. In such situations, it is important to clearly define and communicate who is to perform various Owner duties.

How to Use this Guide

The guide is broken into three sections. Section 1, "Things an Information Owner Must Know" focuses on the responsibilities of the Information Owner role and provides or identifies information an Owner must know in order to effectively execute his/her responsibilities. Section 2, "An Owner's Ten Step Data Protection Plan" provides a suggested process for an Owner to follow to secure data. Use this to systematically execute a plan to secure your data. Section 3, "Best Practices" identifies policies and procedures that an effective Owner will consider when determining the controls to be used to protect information resources for which he/she is responsible. At the end of each section, you will find a checklist tool to help guide you as you perform your Owner responsibilities.

It is expected that some readers will not be familiar with the Information Owner role and its responsibilities, the tasks that an Owner should perform, who to engage for assistance, and some of the best practices for securing data. If this is your situation, you should read the guide from start to finish. Afterwards, use the guide as a reference. Complete the checklists at least once and then review them periodically to ensure that security controls remain in effect over time.

Section 1: Things an Information Owner Must Know

Understand the Importance of Information Security

Students, employees, patients, granting authorities such as the National Science Foundation and the National Institute of Health, and others who provide information to the University, or fund research, expect that information will be properly protected and personal privacy preserved – and rightfully so. As public stewards we have legal, contractual, and moral obligations to protect the information resources of the University and the confidential data of employees and the students and patients we serve. Beyond this, the stakes for failing to secure data are high. A single successful cyber attack against a University of Texas System 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,
- Disruption of patient care, instructional services and administrative functions,
- Loss of reputation for the institution,
- Financial loss to the University resulting from payments of mandated notifications or for providing credit monitoring services to individuals whose personal data has been exposed, and payment of any regulatory fines,
- Increased regulatory oversight,
- Loss of good will and potential loss of donations,
- Loss of grants,
- Loss or corruption of research data,
- Extortion, with University data being held for ransom,
- Equipment malfunctions that can impact University operations or patient care.

Know and Understand the other Information Security Roles

Rest assured, you, as an Information Owner, do not have to become a security expert to meet your security responsibilities and properly secure your data. There are other information security roles defined by state law and U. T. System policy, and there are employees on your campus performing these roles. There are four roles, in particular, with which you need to be familiar. It is important that you understand the relationship between your role of Owner and each of these roles.

- **User:** A "User" is a person (or sometimes a computer program) who an Owner has authorized to access data under his/her authority. Data must be used only for purposes specified by the Owner. Also, Users must comply with any controls specified by the Owner and must prevent disclosure of confidential or sensitive data.

  The Relationship between Owner and User: Working within policies of the institution, the Owner establishes the rules about handling of data under his/her authority and informs Users as to what data they can access, what the data can be used for, and how it must be protected while under the User's control. Users must comply with the Owner's requirements.

- **Custodian:** A "Custodian" is a person or organization responsible for implementing Owner-defined controls and access to data or other information resources. Most often, specialized security tasks are assigned to organizational units such as the Central IT group or a departmental IT group, or to specific individuals within a department. Each of these organizations and individuals serve in the role of Custodian. For outsourced services, private vendors serve as Custodians.

  The Relationship between Owner and Custodian: Within institutional policy, the Owner identifies or selects Custodians to perform IT security functions for the resources under his/her authority. The Owner specifies security controls that Custodians in turn implement and monitor. In other words, Custodians provide services to Owners – you are their customer.

- **Information Security Administrator (ISA):** The ISA is usually a departmental employee who assists the Owner in performing information security tasks, such as required IT risk assessments. Depending on need, some ISAs have IT operational duties within a department or function; others serve more in a role of liaison between the Information Security Officer and the department to exchange information and report incidents. Note that "Information Security Administrator" is a "role" not a job title. ISAs may go by many titles. Whatever the person's title, all ISAs also serve in the role of Custodian because they assist with security related duties.

  The Relationship between Owner and Information Security Administrator: The Owner typically appoints the ISA. In some cases, an Owner may choose to serve also in the ISA role.

- **Information Security Officer or Chief Information Security Officer (ISO):** Each U. T. System institution has a designated individual responsible for establishing and administering the institution's Information Security Program. This person oversees the Information Security Office, establishes policies, monitors systems, investigates incidents, and performs a myriad of other duties related to running an institution-wide information security program. The Information Security Officer is an important resource for Owners. You should confer with the ISO or his/her staff about any questions relating to how to classify information and which security controls would be appropriate for various situations.

  The Relationship between Owner and the Information Security Officer: The Information Security Officer manages the institution's information security program. Owners are required to abide by policies and procedures of the program, report incidents, and cooperate with efforts to assess the security state of the institution. On the flip side, the ISO and staff are Owners' greatest resource in helping determine how best to secure the resources for which they are responsible. You should get to know the ISO and not shy away from asking for help and guidance in performing your security responsibilities.

Know Your Information Owner Responsibilities

As Information Owner your general charge is to classify data, assess risk, specify controls, and ensure agreed upon security strategies are implemented and continue in operation over time. This document will provide guidance to help you with these tasks. Your institution may have a policy that defines the Information Owner responsibilities more precisely. Check with your Information Security Officer.

The state of Texas assigns the following responsibilities to an Information Owner.

- **Approve access to data.** Within institutional policy, the Owner determines by whom and under what conditions data under the Owner's authority can be accessed and used.
- **Review Access Lists.** The Owner periodically reviews access lists to ensure only appropriate people can access data, and in particular to verify that ex-employees have been removed. This task is often delegated, but it remains the Owner's responsibility to see that this is done in accordance with institutional policy or at least annually if no policy exists.
- **Assign custody of data.** Most often, an Information Owner is not the person who handles day-to-day technical activities involved in securing data. Those tasks are usually handled by assigned Custodians. The Owner assigns the Custodian(s). In some cases, Custodians are established by institutional policy.
- **Classify data**. Based on institutional policy and data classification standards, the Owner is responsible for classifying data under the Owner's scope of authority.
- **Specify data controls and convey them to Users and Custodians**. The Owner determines the controls to be used to protect data and communicates this to Custodians and Users. Determining appropriate controls is a task for which most Owners should consult with staff from the Information Security Office.
- **Approve, justify, document, and be accountable for exceptions to security controls.** There may be times when a control required by policy is not appropriate for a given situation. The Owner must approve any exceptions. The Owner must also justify and document why the exception has been granted. The Owner is the accountable party for such decisions.
- **Confirm that controls are in place.** This is perhaps the most important of all Information Owner duties. Too often, people assume that all necessary controls are in place when in fact they are not. The Owner must periodically confirm with Custodians that controls are in place.

Lessons Learned:

- Do NOT assume controls are in place – periodically confirm it. A frequent cause for security incidents is people believing protections are in place when in fact they are not. There have been instances when people assumed data backups existed, only to learn otherwise. Other incidents have occurred when people thought firewalls or anti-virus software were protecting data but learned otherwise.
- Tasks that are measured or on occasion verified are more likely to be attended to than tasks that are performed on good faith alone. The importance of securing your data warrants periodic confirmation that controls that you believe to be in place are working as expected.

University of Texas System policy specifies the following additional Owner responsibilities:

- **Designate an individual to serve as an Information Security Administrator.**
- **Perform an annual information security risk assessment.** In relation to the risk assessment, the Owner also identifies, recommends, and documents, acceptable risk levels for resources under his/her control.

Understand Types of Incidents and the Threat Landscape

An information security incident is any event that results in unauthorized access, disclosure, loss, modification, disruption, or destruction of information resources whether this occurs deliberately or by accident. Consider the following headlines:

Stolen Patient Records Cost University $ Millions - June, 2008: University of Utah backup tapes containing 2.2 million patient records are stolen from a vehicle. The incident occurred because an employee of a vendor who transports and stores backup tapes off-site in a secure storage facility, made the decision to not deliver the tapes directly to the facility. Instead he went home and left the tapes in his automobile from which they were stolen. Cost of the stolen media was approximately $50, but the remediation cost to the University of Utah totaled $3.3 million.

Lessons Learned:

- Failure to execute small security related tasks can have costly consequences. It is critical that day-to-day security operations be performed consistently.
- An institution cannot have total control over what individuals may do. Therefore, it is important to use other preventive measures that one can control. Had the backup tapes been encrypted the impact of the incident would have been minimal.

Blackboard Access Used for Cheating - Spring, 2008: University of Texas at Brownsville investigates cheating made possible because of various access related failures, including misuse of assigned privileges, sharing of access credentials, and inappropriate assignment of access privileges.

Lessons Learned:

- Owners must understand and execute on their information security responsibilities.
- Owners must establish policy relating to access and use of data.
- Owners must understand and fully utilize role-based security and other security features available in the computer applications used to support business functions..
- Owners must understand the threat environment, potential motivations of attackers, and serve as example to others regarding concern about information security.
- Nobody wants to believe an employee would misuse privileges, but it happens; be vigilant!
- Student workers who use email for performing University business must have two email accounts, one for personal use, and another to use exclusively for University business.

Criminals Hold Virginia Patient Data for Ransom - May, 2009: Criminals breach state of Virginia computer systems, encrypt 8.3 million patient records, delete the state's backups, and demand a $10 million ransom for the encryption key. The root cause has not been made public, however, it is speculated that there may have been inside assistance. Outcome? The records were eventually restored. Neither the state of Virginia nor FBI will comment on whether a ransom was paid.

Lessons Learned:

- Be aware of the "insider threat," and to the extent possible implement separation of duties in data center operations.
- For mission critical data, keep some backups off-site in a location not electronically accessible directly from the primary storage location.
- Require two-factor authentication for Custodians who have elevated privileges on devices hosting Mission Critical or Confidential information. (See Section 3: Best Practices)

Patients Warned of Potential Identify Theft - January, 2010: MedAssets, a Georgia company assisting the University of Texas Medical Branch with insurance billing and collections informs UTMB that a MedAssets employee with access to UTMB patient billing records had been arrested and charged with identity theft. Although a background check had been performed during the hiring process, it failed to identify the applicant as a possible problem employee. As a precaution, UTMB sends notification letters to some 1,200 individuals possibly affected.

Lessons Learned:

- In work situations that involve storage of Confidential information, it is particularly important to maintain logs that can track who accesses data.
- Periodically monitor logs to ensure access privileges are not abused.
- Ensure that vendor contracts contain appropriate language to address information security issues and reporting requirements for the vendor in event of a breach.

The above examples are but four of the hundreds of incidents that have occurred over the past few years. Present day security incidents fall into three general categories of Errors and Accidents, Attacks of Opportunity, and Targeted Attacks. Strategies are needed to help prevent each type. Specific best practices will be identified in Section 3 of this guide.

Errors and Accidents: These are unintended events that result from someone making a mistake, failing to perform a task, or because of equipment malfunction. Examples include an event in which a University employee inadvertently sent a document containing sensitive information through email to the wrong mail group. In another example, a mechanical failure caused addresses on letters to be misaligned resulting in exposure of confidential information through the windows of the envelopes.

These type of incidents are unfortunate, but inadvertent and involve no intent for harm. Errors will occur, but they can be reduced by focusing on operational quality controls.

Lessons Learned:

- Use encrypted email when sending confidential information through email.
- Operations that involve confidential information should be thoroughly tested before execution.

Attacks of Opportunity: The most common example, and one often repeated, is a laptop computer being stolen because it was left in view in an accessible location without proper physical controls such as a cable lock. A thief may simply want a new computer, but if a stolen computer happens to also contain confidential data, the data loss can be much more costly to the University than the cost of the computer itself. When a computer disappears, one does not know the motivation of the thief. The institution must treat the event as if the intent had been to obtain any confidential information that may reside on the computer.

Lessons Learned:

- Use physical controls (such as locked doors and cable locks) to secure computers.
- Loss of data on a computer usually poses more risk to the institution than loss of the computer itself. Remove unnecessary data - especially confidential data – from laptop and desktop computers. It exposes the institution to unnecessary risk. Check with your ISO for tools to help you identify this data.
- If you must store confidential data on a laptop or desktop computer, encrypt it using the standards supported by your institution.

Another common “opportunity” incident involves the hacker who simply scans randomly across the Internet in search of unprotected computers. The hacker may be looking for data to use for identify theft or may want to take clandestine control of the computer to send spam or attack others.

Lesson Learned: All computers must be protected from intrusion – even those that do not hold confidential or sensitive information. Any network attached computer under the control of an attacker can be used to send spam, collect data a user types into the computer, or to launch attacks against other computers. It is important to prevent University resources from being used against others.

Targeted Attacks: A targeted attack is one in which the attacker has pre-selected the institution, department, program, or individual to attack. The motivation may be to punish the intended target perhaps for reasons of political or personal vendetta. More commonly, the intent is to obtain data for purposes of personal profit by selling it or by using it directly for identity theft. The motive may also be to gain economic or military advantage. Reports of targeted attacks have become more frequent over

the past eighteen months or so. Universities are at risk of such attacks for three reasons. They store financial data, including social security numbers, that can be used to commit identity theft; they hold vast stores of intellectual property including research data, scholarly works, lecture content, and tests; and they are very complex organizations that rely heavily on interconnected computers and systems. The more complex the environment the more difficult it is to secure, and the more important it is to have automated processes in place to ensure the daily details of securing information are attended to.

A hypothetical example of a targeted attack is a person purposefully obtaining the credentials of an employee known to have access to a course management system for purposes of obtaining test data. Another example would be an attacker who tries to gain access to specific restricted research data.

Lessons Learned:

- Never assume data has little value to others. If it has value to you, it likely has value to others.
- Where possible, simplify operations. Complexity is the enemy of information security, making it harder to understand and protect systems. Take the initiative to understand how your systems work and confirm that protections are in place and remain so over time.
- Operational excellence is of paramount importance! Many incidents occur because a procedure was not followed, or logs were not monitored, or systems were not patched, or device configurations were incorrect, or anti-virus software was out of date. The list goes on. Execution of day-to-day security operations must be consistent and continuous.
- Where possible, automate operational tasks and oversight of those tasks to reduce errors.

Incidents occurring within University of Texas System institutions.

As an Owner, work with your Information Security Office to ensure that strategies are in place to protect against the full range of common threats. Following is a list of the most common security incidents that occur within University of Texas System institutions:

- Stolen or lost computers. Note that a lost computer must be assumed to have been stolen and treated as such in terms of reporting and mitigation.
- Network and server attacks. These attacks typically are launched from a distance, often appearing to come from overseas.
- Application attacks. These attacks also often appear to come from overseas.
- Phishing attacks. Typically, such attacks consist of an email message or a link on a website. The purpose is to trick the user into divulging confidential information (such as a password) that the attacker can then use for other purposes.
- Mal-ware attacks. Malware includes such things as “keyloggers” used for collecting confidential information such as passwords and “bots” that are used by an attacker to remotely control an infected computer for purposes of distributing spam or attacking other computers.
- Misuse of authorizations. Sometimes a University employee or employee of a business partner misuses his/her authorizations.. The motivation may be simple curiosity (e.g. inappropriately viewing the medical records of a patient), to steal information (e.g. obtaining information to commit identity theft), to modify information (e.g. to change a person’s grades), or to destroy information (e.g. a disgruntled employee deleting information that is needed by the institution).

Know Your Computing and Work Environment

Owners must have a holistic understanding of the environment in which work is performed and in which their data is housed and processed. Become familiar with the following:

- **Know your Information Security Officer:** The institutional Information Security Officer is a great resource for you. Do not fret over the technical controls required to protect your data assets – call on your ISO to advise you. Information Security Office staff can assist you in determining the classification of your data and can help you determine what controls are most appropriate for protecting the data. Make an appointment to talk about your data and security concerns. Your call will be welcomed.
- **Know your Data:** All data must be classified. As Owner, you are responsible for this task. Also you are responsible for complying with records retention requirements for the data based on its purpose. As part of understanding your data, it is important that you know which regulations, such as HIPAA, FERPA, or PCI-DSS, your data is subject to. Without a thorough understanding of your data, you do not have the information needed to establish appropriate controls.
- **Know where your Data is located:** Today's interconnected computing environment is very complex. Your data may reside within an institution's data center, on a departmental server, on employee workstations, laptops, home computers, or USB or other portable devices. If you outsource, data may reside in a vendor's computer center that could be located anywhere within the country, or perhaps even overseas. It is imperative that you understand where your data is located! If you do not know this, you cannot protect it.
- **Know how your Data flows:** Data is mobile and has a life cycle. It is created, stored, manipulated, moved, and used in many ways by multiple individuals and functions. And eventually it is archived or destroyed. For the data over which you are responsible it is important that you understand how the data flows. Who creates it, accesses it and uses it? Where and when does it move? What happens to it when its business purpose has been completed – is it destroyed or archived?
- **Know your applications and their capabilities:** You must have a basic understanding of the business applications used to process your data, and you must understand the security capabilities – or lack thereof – of the applications. Understand that applications age. As technologies change applications that may function well from a functional task perspective may in fact pose grave security risks if such applications are used to manage Confidential or Mission Critical Data. These applications should be replaced.
- **Know your Custodians:** Owners assign custody of data to other individuals or organizations to tend to different security functions. It is important that you know who the person or group is that is taking care of such things as: Backing up data, securing servers on which your data is processed or stored, ensuring that laptops are encrypted, and that all computers that may have access to your data are properly secured with up-to-date patches and antivirus software. Often, there are designated groups on campus to perform these tasks, but as Owner you must verify that these tasks are being addressed.
- **Know which controls are in place protecting your Data.** A good initial conversation to have with your Custodians is to ask them how your data is being protected. As you work through this guide and become familiar with best practices, you can verify that current protections are sufficient given the classification and risk to your data.

Checklist for Section 1: Things an Information Owner Must Know

The list below contains items about which all Information Owners should be familiar in order to execute security responsibilities effectively. Place a check by those that you have addressed.

✓	Item
	1. I know who serves in the role of Information Security Officer (ISO) for the institution. (If not, call the Help Desk to inquire.)
	2. I have determined whether the institution has a policy or established procedure for formally designating Information Owners. (Check with the ISO)
	3. I have determined my status as an Information Owner. (See page 1. Confer with your ISO.)
	4. As an Owner, I know if I am in a "Shared Ownership" situation. (Check with your ISO)
	5. Answer only if you are in a "Shared Ownership" situation. I have a clear understanding of who is charged with responsibility for ensuring that the various Owner responsibilities are addressed. (Confer with the other Owners and decide who will perform various tasks (such as classifying data etc.)
	6. As an Owner, I know the responsibilities associated with and my relationship to each of the following Information Security Roles: User, Custodian, Information Security Administrator, Information Security Officer. (See "Know about the other Information Security Roles".)
	7. I know the individuals and/or organizations that serve in a Custodian role for the systems and data over which I have Owner responsibility.
	8. I am familiar with the responsibilities of an Information Owner. (See "Know your Information Owner Responsibilities. Check with your ISO to determine if an institutional policy exists identifying Owner responsibilities.)
	9. I know whether my institution has a "Data Classification Policy" and where to access the document. (Check with your ISO)
	10. I know which regulations my data is subject to, and I am familiar with the requirements? (Check with your Compliance Officer or Legal Counsel.)
	11. I know whether I am required to appoint an Information Security Administrator and/or the identify of this individual. (Check with your ISO)
	12. I have a general understanding of the various types of threats to my data and the types of incidents that can occur. (See "Understand Types of Incidents and the Threat Landscape.)
	13. I know the characteristics of my Data and its classification(s). (See the institutional Data Classification Policy. Check with the ISO)
	14. I know where my data is stored. (Check with your Custodians)
	15. Answer only if you use vendors: I know what data business partners hold and the locations of their data centers. (Check with your vendors. Check any contracts to ensure this conforms to contractual requirements.)
	16. I know where backups of my data are stored. (Check with your Custodians)
	17. I understand the life cycle of my data, including its source(s) and the business rules that govern its flow and eventual archival or destruction. (Check with colleagues including business analysts or systems analysts that maintain systems used to manage your data.)
	18. I know who (which groups) has access to my data and the conditions under which the data is used. (Check with the Custodian charged with oversight of access controls.)
	19. I understand the function of applications used within my business area and know the security features of the applications. (Check with the vendor or the responsible IT group.)
	20. I know which controls are in place to protect my data. (Check with your Custodians and your ISO)

Section 2: An Owner's Ten Step Data Protection Plan

This section provides a step-by-step process which when completed, will put you in good stead in terms of protecting your data and other information resources. If you have not already done so, this would be an excellent time for you to appoint an Information Security Administrator to provide assistance.

The following action plan is written with an assumption that no activities have been performed to date, which is very unlikely. Most University of Texas System institutions already have processes in place for addressing many of these steps and you have likely been performing some, if not all of these activities. The purpose is not for you to re-do activities already performed. If you have a mature program, use this guide to help fill in any gaps between current and optimal practices.

Step 1: Read "Section 1: Things an Information Owner Must Know"

Execution of the steps outlined in this plan presupposes that the reader is familiar with the concepts and roles defined and explained in Section 1 of the guide. If you have not reviewed those materials, it would be beneficial for you to do so before continuing.

Step 2: Appoint an Information Security Administrator (ISA)

Likelihood is that your department or functional area already has an appointed Information Security Administrator, but if this is not the case, you should appoint one. The ISA will work with staff from the Information Security Office. The type of individual you should appoint depends on the nature of the functional area. If you administer a technical function, that perhaps hosts and supports its own computers and systems, the ISA is likely to be a technical employee. In less technical areas, the ISA may have little technical background. In all cases, you should appoint someone who you trust and who can be counted on to report breaches to the Information Security Officer (ISO). This person may serve as liaison for exchange of information with the Information Security Office and will likely assist with completion of annual risk assessments and other security related duties.

Lessons Learned:

- Information Security Administrators must be properly trained for their function. These individuals perform critical security tasks, which if not performed correctly can lead to costly information security breaches.
- A department or function unable to provide or obtain appropriate technical training for the ISA, should not host departmental information systems and data. Those functions should be moved to the institution's central IT organization or be outsourced to an organization capable of providing professional services in a secure environment.

Step 3: Meet with Your Information Security Officer

Make an appointment for you and your ISA to meet with your institution's Information Security Officer or a member of the Information Security Office staff for an initial discussion about your area's information security needs. There are three objectives for this initial meeting. First, you want the ISO to gain a general understanding of your functional area including its missions and business functions, and the data for which you are responsible. The ISO will need this understanding to advise you about protective measures appropriate for your area. Second, use the meeting to inquire about 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. Finally, this is an opportunity to build relationships with the ISO and Security Office staff. When and if problems arise, it is helpful to know the individuals you will be calling on for assistance. Get to know these individuals so you will be comfortable calling with questions as you progress through the process of securing your data.

Step 4: Inventory your Information Resources Assets

Within University of Texas System institutions, multiple security incidents have occurred involving exposure of information contained in data files that the Owner did not know existed. In at least one case, exposure of a previously unknown file resulted in thousands of notification letters having to be sent to affected individuals. This costly exposure involved a file that was many years old and of no use to the institution. The file should have been purged years before. In another case, a server that the organization did not know existed was successfully attacked. An inventory of resources is an important building block for establishing a secure environment.

Lessons Learned:

- It is exceedingly difficult to protect assets and the data they may hold if the Owner does not know the devices or data exists.
- In accordance with the institution's records retention schedule, destroy data that is no longer of use to the University.

Within your scope of responsibility, maintain inventories of the following:

- **Data:** This consists of a list of the data for which you are responsible, the classification of the data, its location, and the Custodian(s) assigned to manage and protect the data. Include backup and test files if they exist; these can pose as much risk to the institution as the production files. If you permit data to be extracted to be used on desktops, laptops, or other devices, include these in the inventory.

Lessons Learned:

- Do not overlook paper documents. These also pose risk. U. T. System institutions have experienced several significant incidents resulting from loss or theft of paper records.
- Work with your institutional Records Manager to purge unneeded paper records.

- **Applications:** This is a listing of computer applications for which your department or function is responsible. Include the version number, vendor, maintenance renewal date, and the Custodian responsible for maintaining the application. Many applications (email for example) are used by multiple departments. Typically, shared applications are included only on the inventory of the department responsible for payment of the licenses and maintenance.
- **Servers:** Keep a list of any server computers that are owned by your department or function. Document the purpose for each server, its age and maintenance renewal dates, and the Custodian(s) responsible for maintaining and securing the device.
- **Other Computing Devices:** This would include desktop and laptop computers assigned to departmental employees and any other networking or computing devices for which your area is responsible.
- **Custodians:** This consists of a list of individuals or organizations that you have assigned responsibilities for managing or securing information assets, or that have these responsibilities because of institutional policy. Include any vendors with which you may have contracted for services. You can use this list to record dates on which you or your designee met with the Custodian to review security controls.
- **Contracts and Service Agreements:** This consists of a simple list of contracts, the purpose of each, the parties, start dates, expiration dates. Review the list periodically to ensure that contracts are renewed as needed well before expiration dates so there are no service disruption that may pose risk to the institution.

All items noted above have an impact on the state of security. You must know what exists in the environment in order to determine appropriate protections. Contracts and service agreements should be reviewed to determine if proper security provisions are included. If an agreement does not contain proper protections, it should be revised to include these protections at time of renewal or extension. Some, if not all, of the suggested inventories probably exist because of other state and University requirements such as annual inventory of assets and annual state required risk assessments for systems that are mission critical or which contain confidential information.

Step 5: Classify your Data

Information Owners are responsible for classifying data under their authority in accordance with institutional data classification standards. Obtain a copy of your institution's Data Classification Policy or standard for guidance. If you are unable to locate a Data Classification Policy, contact your Information Security Officer.

If you determined that no such policy exists, you should, at minimum, identify data that is Confidential which the state defines as, "Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements)." Classify data as "Confidential" (based on the above definition), "sensitive" which would include most

other data, or “public” which, for this purpose, would be data intended for the public such as data on the institution’s website.

Step 6: 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. Establish a policy that codifies these requirements. The policy establishes the ground rules for how data is to be accessed, modified, and used. The policy is needed for training of Users and for working with Custodians to implement access controls.

Note, whether a specific access control policy is needed for your department or function depends on the nature of the function. The institution may have an overarching Access Control Policy that is sufficient to meet the needs of your unit. However, if your department or function creates or stores data unique to the function there may be a need for a supplemental policy. Also, if you allow data to be downloaded you should specify who is to be allowed to download, the conditions under which this is allowed, permitted uses of downloaded data, and the disposition requirements for the downloaded data once its purpose has been served.

Step 7: Specify Controls and Identify/Select Custodians

Having classified your data, and with inventories and access policies in hand, you are ready to meet with the ISO or his/her staff to decide on controls appropriate for your circumstances. **Use the information found in “Section 3: Best Practices” as a structured approach for discussing these controls.** 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. Select and meet with each Custodian (individual or organization) to ensure that it is clearly understood as to which services are being provided and by whom. Make sure that all desired protections have been assigned. The Section 3 checklist can be used to document controls.

Step 8: 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 University 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! A department comprised of employees who are security conscious is less likely to experience a security incident than one comprised of employees who pay little heed to security.

Lessons Learned:

- Administrators who value and demonstrate thorough word and action that information security is important help instill these attitudes in their employees.
- Many information security incidents result from employee error and in some cases neglect. Such incidents are less likely to occur in departments in which employees value and are mindful of information security.

Following are strategies that you can use to consistently demonstrate the importance of information security to staff in order to build a security minded culture.

- Establish departmental (or function) access control and data use policies.
- Provide information security training for your employees that focuses on security issues relevant to your area.
- On occasion, include information security as a topic during department meetings.
- Invite staff from the Information Security Office to perform an assessment of physical security in your area and address security weaknesses identified.
- Invite the Information Security Officer to speak at a department meeting to discuss information security issues relevant to your institution and area.
- Send news articles concerning information security and breaches to staff.

Step 9: Perform an Annual Risk Assessment

For many years, state regulations have required that a risk assessment of information resources be conducted annually for high risk resources and every two years for all other information resources. More importantly, risk assessment is a required process for determining where to place protections and allocate resources security resources. It is a mistake to under protect your resources, but it is also costly and ineffective to over protect.

You have most likely already performed an IT risk assessment. If so, this step is simply a continuation of your current practice. If you have not previously participated in an annual risk assessment, contact your Information Security Officer and inquire about your institution's process to ensure your area is included in future assessments. Use results from your risk assessment as another source for determining which security controls to implement.

If you learn that your institution does not have an established procedure for performing risk assessment, ask when one will be in place. If the time-frame does not meet your needs, contact the U. T. System Office of Information Security Compliance at ciso@utsystem.edu for assistance in performing an independent assessment for your functional area that can be used until the institution establishes a formal process.

Lessons Learned:

- Following a breach, it is common to learn that no risk assessment had been performed on the system or in the department in which the breach occurred. Risk assessments help identify vulnerabilities that can help prevent incidents.
- Participation in an annual risk assessment has proven to be an effective method for raising general awareness about information security concerns within a department.

Step 10: 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. An optimal timeframe for doing this would be twice per year, but at minimum you should complete the following tasks annually.

- Review, or ask your ISA to review, the access rules for your systems and data. Review access lists and confirm that access groups include the correct individuals and that roles are correctly defined with proper access rights assigned. Confirm that no former employees continue to have access to data. Be sure also to review lists that identify the individuals who have remote access to information systems and data.
- Meet with each of your Custodians and confirm that your specified controls are still in effect. Ask for documentation that would indicate the state of the control and keep this documentation on file. Custodians are people also, and they can make errors. Verification is in your best interest, and also the best interest of the Custodian.

Lesson Learned: Do not assume, simply on reputation, that a Custodian has all essential controls in place. It is important to be vigilant and confirm controls. As an example, the state of Texas contracted with IBM – no small player in the IT world - to the sum of $863 Million to consolidate data centers and secure agency data. However, a server failure caused need to restore data only to reveal that poor backup processes were in place resulting in temporary data loss of Medicare fraud investigation information. Some data was never recovered.

Checklist for Section 2: An Owner's Ten Step Data Protection Plan

Use this checklist to track execution of your Data Protection Plan. Mark the steps and items as they are completed.

✓	Action
	Step 1: I have read "Section 1: Things an Information Owner Must Know."
	Step 2: An Information Security Administrator (ISA) has been appointed for my area.
	Step 3: I have met with the Information Security Officer.
	Step 4: All Inventories have been completed.
	Data Inventory Exists.
	Application Inventory Exists.
	Server Inventory Exists.
	Inventory of other Computing Devices Exists.
	List of Custodians Exists.
	Inventory of Contracts and Service Agreements Exists.
	Step 5: Data under my Ownership has been Classified.
	Step 6: Data Access Policy Exists.
	Step 7: I have specified controls and Identified/Selected Custodians to implement the controls.
	Step 8: I am working to establish Information Security as a Value within my functional area.
	I provided (or arranged for) information security training regarding department issues.
	I included information security as a topic in department meetings.
	I had Information Security Office staff perform an assessment of physical security.
	The Information Security Officer has spoken at a department meeting about security issues relevant to the department and institution.
	I have sent news articles concerning information security and breaches to staff.
	Step 9: I performed a risk assessment within the past year.
	Step 10: Confirm that Controls Remain in Place.
	I have conducted an initial review of access control lists to ensure only appropriate people are authorized for access.
	I have reviewed and confirmed with all Custodians that intended controls are in place and functional.

Section 3: Best Practices

Lesson Learned: To protect information resources, Owners should adopt best practices. Be careful to not merely mimic common practices. The information technology landscape changes quickly; yesterday's best solution is likely not today's. For example, anti-virus software, once a universally accepted "best practice" has lost much effectiveness given today's zero-day malware threats. Confer with your Information Security Officer and others who have special knowledge about information security when determining the controls you will use.

Specifying protective controls is an important Owner responsibility. Review with your Custodians the controls that are currently in place, your needs, and any changes that you believe may be warranted. Custodians can provide insight and advice, but you remain responsible for the business function that will suffer in event of an incident or breach involving your data. Therefore, it is important that you understand the existing controls and their function, and determine if controls need to be removed, changed, or added. In this section, you are presented with controls that have proven to be effective. They are best practices. The purpose of each control is given, along with other relevant comments about its potential for use within University of Texas System institutions.

As you review recommended practices, keep in mind that this is by no means an exhaustive list of best practices. This list is based on observations and situations that have occurred or are known to exist within the U. T. System that indicate need for adoption of improved practices in some areas. Many of these practices will likely already be in place at your institution. However, if gaps are identified, discuss these with your Information Security Officer and any other Custodians from whom you receive services to determine if there is need for changes to current practices.

Keep in mind that decisions about controls to deploy should be based on assessment of risk. Protect your systems and data according to the risk that their exposure, loss, destruction, or misuse poses to your operations and to the University. Also, understand that there may be alternative methods for addressing risks. The mere fact that a control listed in this guide is not being used, does not in itself indicate a security weakness. The control may not be needed because risk is very low, or alternative protections may be in place. The point is that you, as an Information Owner, must understand how your resources are being protected and determine if protections are adequate.

Control Types

Within the information security profession, controls are typically categorized as "Management Controls" (also referred to as Administrative Controls), "Physical Controls," and "Technical Controls." As an Owner, you will want to ensure that all three types of controls are used to secure your environment and information resources.

Management Controls: These include policies, procedures, personnel practices, and training that the institution and you establish to protect program resources. These define the rules and processes for securing program resources. Management controls define who and under what conditions data may be accessed and used and required training.

Physical Controls: Included here are devices such as locks, cameras, etc. used to preserve the physical security of computers and other computing devices and the data stored on those devices. Physical security is not complex to understand, but diligence is required in order for it to be effective.

Technical Controls: Here are the software and hardware devices used to protect data and monitor the environment. Anti-virus software, network firewalls, and intrusion detection/prevention systems are examples of technical controls.

Lesson Learned: It is not uncommon for an organization to focus too much on a single type of control – often the technical controls, at the expense of others. An effective security program requires a holistic approach. A Technical Control such as role-based security capabilities built into an application provides little value if the policy structure is not in place to identify who should be assigned various roles and the access levels to be associated with each role. The Management Control is required to provide direction on use of the Technical Control. Also, no computer firewall is capable of preventing an individual from walking in and stealing an unsecured computer off of someone's desk. Physical Controls are very important.

Best Practices Matrix and Checklist

On the following page is a matrix of best practices identified as having been relevant to incidents that have occurred within the University of Texas System with which Information Owners should be concerned. Discuss the identified controls with your Custodians. In consultation with Custodians, use the matrix initially to determine the controls to be used for protecting your function's information resources and data. Document controls that are already in place and identify those to be added. Add lines as necessary to document controls that are not pre-populated.

EXAMPLES:

In place? ✓		Control	Assigned Custodian	• **Category** • **Control Type** • **Comments** • **Documentation of Custodian Discussion.**	Date last confirmed in place.
✓		Place servers in secured, professionally run data centers.	Central IT Group	Category: Server Administration Control Type: Physical Control Comments: Servers need to be protected from theft, vandalism, or breach. Documentation: We decided to move all our servers to the Central IT server room.	2/5/2010
✓		Conduct Annual 3rd Party Penetration Test	Information Security Office arranges for an outside vendor to perform the assessment.	Category: Network & Server Security Control Type: Technical Control Comments: This provides an unbiased outside assessment to double check work of the institution and to provide added credibility to the effectiveness of security controls. Documentation: All findings were addressed.	6/24/2010
		Create and Adopt Access Control Policy for Departmental Data	Information Owner and Department Staff	Category: Access Control Control Type: Management Control Comments: Projected completion: 12/31/10 Documentation: The policy will identify and define roles, and determine which access and modification rights are assigned to these roles.	

Best Practices Matrix and Checklist

In place? ✓	#	Control	Assigned Custodian	• Category • Control Type • Comments • Documentation of Custodian Discussion.	Date last confirmed in place.
	1	Place servers in secured, professionally run, data centers.		Category: Server Administration Control Type: Physical Control Comments: Servers must be protected from theft, and vandalism. They require redundant power feeds and environmental controls for reliability. Ask your Custodian: Where are my servers and data located? What physical security controls are in place to protect them? Documentation:	
	2	Change default passwords on servers following initial installation and periodically change them afterwards.		Category: Server Administration Control Type: Management and Technical Control Comments: Default passwords are known by IT professionals making it easy for an attacker to guess. Ask your Custodian: Have default passwords been changed on the servers hosting my applications and data? What was the date on which the passwords were last changed? Documentation:	

	3	Server Configuration Management Software		Category: Server Administration Control Type: Technical Control Comments: Servers must be properly configured and patched to be secure. This software allows the Security Office to confirm the security state of servers. Ask your Custodian: How are server configurations and patches managed? How do you verify that servers are configured properly? How do you verify that configurations remain as desired over time? Does the Security Office have visibility into server configuration? If not, how do they confirm configuration and patch status? Documentation:	
	4	Log Monitoring		Category: Server Administration Control Type: Management Control Comments: Logs identify successful and failed access attempts and can be used to determine if unauthorized access has occurred. Ask your Custodian: to describe the process for monitoring server logs. Ask if the logs being kept are capable of identifying actual access to data in addition to logon attempts. Documentation:	
	5	Server Administrator Qualifications and Training		Category: Server Administration Control Type: Management Control Comments: Unqualified administrators can fail to perform needed tasks and are more likely to inadvertently mis-configure devices, leaving them vulnerable to attack. Ask your Custodian: What qualification and certifications do you require of server administrators? What training do you provide for them? What “security” training do they receive? Documentation:	

	6	Use formal Memorandums of Understanding (MOU) or Service Level Agreements (SLA) to clearly define who is responsible for performing server (and other) related security tasks.		Category: Server Administration Control Type: Management Control Comments: A MOU or SLA documents who is responsible for performing tasks to ensure that all security tasks are assigned and known to the responsible party. Insist on execution of a SLA or MOU that clearly assigns security tasks. Documentation:	
	7	Require Two-Factor Authentication for Administrator Access to Servers		Category: Management and Technical Control Control Type: Access & Server Administration Comments: Two-Factor authentication requires use of an ID and password plus a token or biometric (i.e. fingerprint etc.) to gain access to the server. It is an effective means for preventing access by unauthorized parties. Ask: Do server administrators use Two-Factor authentication? Documentation:	
	8	Perform background checks on all employees (including work-study students) and Custodians who will have access to student records or other Confidential information.		Category: Access Control Type: Management Control Comments: Custodians and employees who have access to sensitive information are in positions of special trust. Ask your Custodian: Do you conduct background checks on all employees? If not, what determines who does and does not receive a background check? Documentation:	
	9	Implement “Need to Know” Access Control Policies that Define Roles and Privileges.		Category: Access Control Type: Management Control Comments: To protect security of data and privacy of individuals, data should be available only those who need to use it to perform job duties. For data that is Confidential or sensitive, does policy appropriately restrict access to those with a business need to know? Documentation:	

	10	Issue and require use of separate credentials and email accounts for student workers. Require all official business - and only official business - be conducted using the employee role credential.		Category: Access Control Type: Management Control Comments: To avoid FERPA and possibly other regulatory violation, official business should not be intermixed with a student-worker's personal email. Documentation:	
	11	Configuration Management for desktop and laptop computers.		Category: End-point Security Control Type: Technical Control Comments: Desktop and laptop computers must be configured properly and patched regularly to maintain a secure state. Configuration management allows the verification to be automated and gives the ISO visibility into the security state of devices across the enterprise. Ask the ISO: Do you have visibility into the configurations of the devices for which I am responsible? How do you verify that desktop and laptop computers are configured correctly? Documentation:	
	12	Use Whole Disk Encryption on laptop computers and desktop computers that process confidential information.		Category: End-point Security Control Type: Technical Control Comments: As computers have become smaller they have become easier to steal. If a stolen computer storing confidential information is encrypted with verifiable whole disk encryption, the data is secure from access and a serious data exposure has likely been avoided. Ask: Are computers that hold confidential information encrypted using centrally managed whole disk encryption software? Documentation:	

	13	Confidential Data Removal		Category: End-point Security Control Type: Technical Control Comments: Computers often contain confidential information that the User is unaware exists. Often this information is no longer of business use, but it continues to pose risk of exposure. Exposures of such data have occurred in U. T. System institutions. Note: U. T. Austin makes available the SENF data discovery tool at no cost. Ask the ISO if your institution has a tool and process for discovery and removal of unneeded confidential information. Documentation:	
	14	Use Application Whitelisting to protect servers, desktop, and laptop computers that hold or process Confidential information.		Category: End-point Security Control Type: Technical Control Comments: With emergence of today's sophisticated zero-day attacks and stealth malware, anti-virus software has lost some effectiveness. It should be supplemented with whitelisting in areas in which confidential data is processed to prevent malware that may find its way onto the computer from executing. Ask your Custodian: How effective is the anti-virus software being used on servers and desktops? What additional measures are in place to prevent execution of malware? Documentation:	
	15	Secure computers with cable locks or other physical devices (locked doors etc.) to prevent theft.		Category: End-point Security Control Type: Physical Control Comments: Many incidents are the result of simple theft. Simple physical measures can be effective in preventing crimes of opportunity that may result in considerable cost to the institution. Documentation:	

	16	3rd Party Penetration Testing		Category: Network Security Control Type: Technical Control Comments: Hire a qualified 3rd party to periodically attempt to access servers from the Internet. This can be used as a means of double checking vulnerability testing performed by the institution. A 3rd party confirmation of controls adds credibility to the institution's assertion of being secure. Ask the ISO the date of the last 3rd party penetration or vulnerability test. Ask if all identified vulnerabilities that might affect your servers were addressed. Documentation:	
	17	Communicate in writing with your Custodian regarding the data files, databases, etc. that are to be backed up and the schedule for those backups.		Category: Data Backup Control Type: Management Control Comments: Failure to have a backup of data when needed is a relatively common error. Ask your Custodian: Which of my data is being backed up? How often are these backups performed? How long are backups kept? Where are they located? How can this be verified? Documentation:	
	18	Encrypt backups that will be transported to another site.		Category: Data Backup Control Type: Technical Control Comments: Lost backup media that contains confidential information presents a considerable risk because, in terms of regulatory response, the media must be treated as if it has been stolen. Ask: Are backup tapes (or other media) encrypted? Documentation:	

	19	Application Scanning		Category: Application Security Control Type: Technical Control Comments: Many breaches are result of applications having not been written with appropriate security coding techniques. Ask: Have my applications been scanned to identify security weaknesses? Do you have a policy relating to when applications are to be scanned? Documentation:	
	20	Contract Review for Security Provisions		Category: Purchasing and Contracting Control Type: Management Control Comments: Older contracts most likely do not contain adequate language to ensure protection of University data. Review these at renewal. Ensure that all renewed and new contracts contain appropriate language. Documentation:	
	21	Vendor Product/Service Risk Assessment		Category: Purchasing and Contracting Control Type: Management Control Comments: When contracting with a vendor for products or services that process University data, perform a risk assessment to determine if the product has appropriate security controls. If data is being hosted offsite, assess the security practices of the vendor to determine if appropriate protections are in place. Documentation:	

	22	Intrusion Prevention/Detection		Category: Network Security Control Type: Technical Control Comments: Processes need to be in place to monitor network traffic and device behavior to determine if an intrusion is being attempted or has been successful so that mitigation can be performed quickly. Ask: Are my systems protected by IPS or IDS? How are alerts identified and addressed? Who receives the alerts and within what timeframe? Documentation:	
	23	**USE THE FOLLOWING ROWS TO ADD CONTROLS THAT ARE CURRENTLY IN PLACE OR THAT YOU AND YOUR CUSTODIANS DETERMINE SHOULD BE PUT INTO PLACE. ADD ROWS AS NEEDED.**		Category: Control Type: Comments: Documentation:	
	24			Category: Control Type: Comments: Documentation:	
	25			Category: Control Type: Comments: Documentation:	
	26			Category: Control Type: Comments: Documentation:	
	27			Category: Control Type: Comments: Documentation:	