Information Security
It’s Everyone’s Responsibility

The University of Texas at Dallas
Information Security Office (ISO)
Information generated, used, and/or owned by UTD has value. Because of this, UTD must be prepared for security threats and possible disruptions of service.

Several federal and state laws, as well as UT System and UTD policies are intended to help protect our data.

Every UTD employee is responsible for learning more about information security and participating in risk reduction.

As an employee, you are often the first line of defense protecting valuable information attackers will try to compromise.
Why do we have an Information Security Office (ISO)?

Mission Statement

The Information Security Office supports the mission of UTD by building a culture of security awareness and risk management to protect the confidentiality, integrity, availability, and accountability of information assets.

The Information Security Office serves UTD as a partner and educator. Risk mitigation is achieved through awareness training, technology solutions, inclusion of security controls in new projects, and regulatory compliance.
Risk Management

ISO’s approach is to **effectively manage risks**, not eliminate risks. Attempts to fully eliminate risks are costly and could cause a disruption in service.

It is important to remember to include ISO in conversations across campus to ensure we build a culture where information security risks are discussed and are at an acceptable level.

ISO’s main goal is to help UTD find ways to conduct business while remaining responsible stewards of information.
Revised Policy

The Information Security and Acceptable Use Policy has been updated!

Thanks to feedback from campus leaders, an updated policy has been established which replaces older documents about Information Security.

To read the entire policy or get more information about particular topics in this presentation, visit the Policy Navigator: http://policy.utdallas.edu/utdbp3096
The term “information security” means different things to different audiences, so let’s begin by defining the objectives:

**Confidentiality**
Users should only see information needed to do their jobs.

**Integrity**
Information should not be altered unexpectedly.

**Availability**
Information should be available to users when needed and systems should perform as expected.

**Accountability**
It should be clear who accessed information, what was performed, and when it happened.
UTD Data vs. Personal Data

Security controls are required in some cases, but only suggested in other situations. Data classification simplifies the selection of security controls.

Personal Data is sometimes associated with Incidental Use. Incidental Use is defined as occasional personal use of UTD Information Systems.

<table>
<thead>
<tr>
<th></th>
<th>University Data</th>
<th>Personal Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires Classification</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Security Controls Required</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Security Controls Suggested</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
Examples of Security Controls

- Data classification
- Encryption
- Users provided only necessary access
- Malware prevention
- Physical security

- Event logging
- 2-Factor authentication
- Personalized usernames for each user

- Access control
- File hashing
- File backups / version history

- File backups
- Disaster recovery
- Malware prevention
- Network storage instead of C drive
Data Classification

UTD data is classified into three categories based on the confidentiality of the data. Recommended methods of protecting data are associated with each category, thus simplifying the process of securing UTD data.

Confidential Data (formerly Category 1) - The subset of University Data that is private or confidential by law or otherwise exempt from public disclosure and/or other University Data about an individual likely to expose the individual to identity theft.

Examples:
- Social Security Number
- Visa numbers
- Drivers' license number
- Student grade information
- Certain research data

Controlled Data (formerly Category 2) - The subset of University Data that is not created for or made available for public consumption but that is subject to release under the Texas Public Information Act or other laws.

Examples:
- UTD-IDs
- UTD Emails
- Files stored on UTD systems (that do not contain Confidential Data)

Public Data (formerly Category 3) - The subset of University Data intended for public consumption.

Examples:
- Published articles
- Information on public websites
- Press releases
- Marketing materials
Encryption Can Be Confusing

Encryption is one of the most important controls to protect confidentiality.

*How does it work?*

Encryption uses special mathematical equations to make data unreadable if it falls into the wrong hands. Only the authorized users are able to reverse the calculation.

*Where is encryption helpful?*

- Encrypting a computer’s hard drive can protect all of the contents in the event that it is stolen.
- Using a LOK-IT removable USB drive, available from the ISO, protects data in the event that the device is lost or stolen.
- Digital certificates can encrypt emails between UTD users.
- Adding “[encrypt]” to the subject line of email prevents attackers on the Internet from observing the email while it is transmitted between organizations.
- VPN remote access protects network traffic while transmitted over the Internet.

For assistance with encryption, email ISO at infosecurity@utdallas.edu, or call extension x6810.
Encryption and Travel

If you plan to travel outside the United States you should know that:

- Some countries will **not** allow entry with encrypted devices.

- Countries who have signed the Wassenaar agreement **DO** allow entry with encrypted devices. A listing of these countries can be found at [http://www.wassenaar.org/participants/index.html](http://www.wassenaar.org/participants/index.html).

- ISO has a limited number of unencrypted laptops that can be loaned to employees traveling to countries that do not allow encrypted devices.
ISO Services

ISO offers many services to help UTD manage information security risks. Some new services offered are:

**Partnership with Box.com for secure cloud storage**
- Use Box.com to store large files, share files outside of UTD, collaborate with teammates, and access files from tablets and smart phones. For more information, please contact the ISO at infosecurity@utdallas.edu or by calling x6810. **If you would like to use a different provider please check with ISO; only Box.com may be used to store data requiring HIPAA compliance.**

**Online Check Out tool for employee transfers and terminations**
- The Check Out tool is available for departments to use to ensure computer access is promptly changed or removed for transferring or departing employees. This is a very important part of ensuring UTD information is protected. [https://isapps.utdallas.edu/CAR/CCU_loginform.cfm](https://isapps.utdallas.edu/CAR/CCU_loginform.cfm)
Vendor Evaluation

UTD business partners may need access to UTD data to perform their services. To ensure their partnership does not introduce unnecessary risk, ISO assists in the evaluation process.

– Potential business partners must complete a Vendor Evaluation form.
– ISO reviews the responses to identify potential risks associated with the vendor.
– ISO meets with stakeholders to ensure the associated risks are understood before a contract is finalized.

You can learn more about the process and access the Vendor Evaluation form: http://utdallas.parature.com/link/portal/30075/30104/Article/660/How-do-I-involve-Information-Security-when-evaluating-a-new-vendor
Because everyone contributes to security...

All UTD employees help protect information when they follow these recommendations:
Secure your Behavior

• Protect your passwords. Attackers try to get passwords via phishing emails, calls, texts, or in-person conversations.

• If you have a guest that only needs access to the Internet, use the Guest wireless network (NetID is not required).

• If you have a guest that needs access to UTD resources, request access by completing a Computer Access Request (CAR) form (your guest will need a NetID to access UTD resources).
Secure your Desktops and Laptops

- Ensure software updates are kept current. Many departments are now using Secunia which updates automatically and allows the efficiency of a single control window. Local technicians and the ISO can provide more information on Secunia.
- Ensure anti-malware software and the latest definitions are installed on all desktops and laptops, regardless of operating system (OS).
- Install whole disk encryption on desktops and laptops – this will protect data stored on the hard drive in the event the device is physically stolen.
- Use network drives rather than local hard drives for storing valuable data. Network drives have a higher level of security and are backed up regularly, preventing data loss in the event your local hard drive crashes.
ISO strongly recommends that you use UTD-owned devices to conduct UTD business. However, if you choose to use a personally owned device to conduct UTD business involving confidential data, it should be protected with the following:

- Strong, unique passwords
- Current software patches, including anti-malware updates
- Whole disk encryption

To better understand the expectations for using personal devices on the UTD network, please review the [Information Security and Acceptable Use Policy](#).
Secure your Mobile Devices

Mobile devices, such as tablets and smartphones, have become essential tools for employees at UTD. Below are some best practices for mobile device security:

1. Lock device after inactivity, with a password or pattern
2. Auto wipe after 10 unsuccessful login attempts
3. Activate tools for remote erase and geographic location of lost or stolen devices
4. Disable Bluetooth when not in use
5. Keep software updates and patches up to date on all devices

For more information about your specific device model, visit the manufacturers website, email ISO at infosecurity@utdallas.edu, or call extension x6810.
Physical Security

Physical security is often overlooked. Failure to ensure physical security can lead to information risks.

Here are some tips for ensuring physical security in your work area:

• Ensure all paper copies of valuable data are locked when they are not in use.
• If you work in an office, ensure you lock the door when you leave. If you work in a cubicle environment, ensure you lock cabinets and bins when you leave.
• Be aware of people wandering in your work space, especially if you work in a restricted area. Never allow someone into a restricted area until authorization has been verified.
• When traveling, UTD assets should be stored where they will not be observed by potential thieves.
Reporting Information Security Incidents

• What is an “incident”?
  – An incident includes events that could lead to accidental or deliberate exposure of data or disruption to security controls.
  – Incidents are investigated by specialists to confirm the causes and possible impact.
  – Examples include a compromised password, a stolen laptop or smartphone, or a computer infected with malware.

• How do I report incidents?
  – Stolen devices should be reported to the UTD Police first, then to the ISO.
  – Compromised passwords, infected computers, and other incidents involving data can be reported to the ISO at infosecurity@utdallas.edu or by calling x6810.
  – You may also contact the Ethics & Compliance Hotline: http://www.utdallas.edu/audit-compliance/hotline/
Thank you for taking the time to review this information.

Want to learn more? Check out our free security awareness classes!
https://utdallas.edu/infosecurity/awareness-training/

To request copies of our informative brochure or to let us know how we are doing, email us at infosecurity@utdallas.edu


You can also visit us on Facebook: https://www.facebook.com/UTDInfoSec

View the complete Information Security and Acceptable Use Policy: http://policy.utdallas.edu/utdbp3096
Congratulations! You’ve completed the Information Security module!

This training module will remain available at the Office of Institutional Compliance website.

<table>
<thead>
<tr>
<th>If you have questions</th>
<th>Anti-virus Software for Home Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact the Office of Information Security</td>
<td>• Download software</td>
</tr>
<tr>
<td>• <a href="mailto:infosecurity@utdallas.edu">infosecurity@utdallas.edu</a></td>
<td></td>
</tr>
<tr>
<td>• 972-883-6810</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classes &amp; step-by-step instructions</th>
<th>Laws &amp; Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Free training classes</td>
<td>• State of Texas TAC 202</td>
</tr>
<tr>
<td>• Mobile device security</td>
<td>• UT System UTS 165</td>
</tr>
<tr>
<td></td>
<td>• UT Dallas utdallas.edu/infosecurity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traveling outside the U.S.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• List of countries that allow encrypted devices</td>
</tr>
</tbody>
</table>