Identity Finder helps you find restricted information stored on your computer. Identity theft can occur when personal information, such as social security numbers and credit card numbers, fall into the wrong hands. For more information on the application and how to install and run it visit: http://its.uiowa.edu/identity/ 

UI Anywhere
A Virtual Private Network (VPN) at The University of Iowa

If you are working from home accessing and using institutional data with systems on campus, do so via the University’s VPN service (UI Anywhere). Instructions on how to install and use the application to securely access UI campus resources can be found here: http://its.uiowa.edu/vpn

Resources for more information

Sensitive/ Protected Data: http://itssecurity.uiowa.edu/policy/policy-InstitutionalDataAccess.shtml
http://itssecurity.uiowa.edu/bestprac/InstData-Classification.shtml
http://its.uiowa.edu/encryption

Cloud Computing: http://its.uiowa.edu/cloud

Incident Response: http://itssecurity.uiowa.edu/incidents/incidents.shtml

Workplace Best Practices: http://itssecurity.uiowa.edu/bestprac/workplace.shtml

ITS Help Desk
Phone: 319-384-4357
E-Mail: helpdesk@uiowa.edu
Web: http://its.uiowa.edu/helpdesk
This “Check List” is intended primarily for UI-owned, self-managed workstations or devices. Use it as a means of assessing your information security and to identify areas you can improve. More checked boxes means less risk.

**Work with your local IT support person if you need any clarification or assistance.**

### Computer/ System Security Requirements

- I keep my operating system and application software patches up-to-date.
- I regularly (at least monthly) check my programs for out of date software and update accordingly.
- I have anti-virus software installed, set to automatically update and scan my system regularly.
- I use complex passwords (University Password Policy) to protect my computer(s), devices, & applications and never share them with anyone.
- I manage and protect my encryption keys (key escrow).
- All of my important information is stored on my home (H:) or on my department shared (L:, S: etc.) drive space, which is backed up.
- I have discussed with my supervisor and completed training requirements related to my position. Examples of training could be, FERPA, HIPAA or Security Awareness.
- I have my firewall configured and activated on my device(s).
- I do not use an account with elevated access for my day-to-day work (i.e. Administrator Account).
- I consult with my IT Support staff or HelpDesk before purchasing or using any cloud based application.
- I ensure and have appropriate licenses for all software and applications installed and running on my machine(s).

### Sensitive/ Protected data

- I know what restricted (Level III) or protected (Level II) data is.
- I store high sensitivity/restricted (University Level III) information on a secure department file server (or within university web applications), instead of locally on my workstation, laptop, tablet, or other mobile device.
- If I must store Level III information on a workstation, laptop, tablet, or other mobile device, I work with my local IT support staff to implement encryption on the device.
- I always use secure end-to-end encryption (e.g., “https” for web sites, “sftp” for file transfers) when communicating any sensitive information.
- I know which files I work with that contain restricted (University Level III) information, and where those files are stored.
- I regularly run the Identity Finder software program on my desktop to ensure it doesn't store any social security, credit card numbers or passwords.
- If Identity Finder flags files with Level III data, I promptly delete, edit, or move them to a secure location.
- I do not share restricted or protected institutional data without appropriate authorization from the business owner for that data.

### Sensitive/ Protected data

- I know what restricted (Level III) or protected (Level II) data is.
- I store high sensitivity/restricted (University Level III) information on a secure department file server (or within university web applications), instead of locally on my workstation, laptop, tablet, or other mobile device.
- If I must store Level III information on a workstation, laptop, tablet, or other mobile device, I work with my local IT support staff to implement encryption on the device.
- I always use secure end-to-end encryption (e.g., “https” for web sites, “sftp” for file transfers) when communicating any sensitive information.
- I know which files I work with that contain restricted (University Level III) information, and where those files are stored.
- I regularly run the Identity Finder software program on my desktop to ensure it doesn't store any social security, credit card numbers or passwords.
- If Identity Finder flags files with Level III data, I promptly delete, edit, or move them to a secure location.
- I do not share restricted or protected institutional data without appropriate authorization from the business owner for that data.

### Work Area Security

- I make sure my computer’s screen is password locked while I am away from the device.
- I secure restricted information on any media (e.g., paper, electronic, including USB drives and DVDs), locking them up in a desk drawer or file cabinet.

### Responding to Incidents

- If I suspect I have a security issue with my computer, I know I have to contact the Information Security and Policy Office (5-6332) immediately, before I do anything on my computer.
- If I have a problem with my HawkID, I know to contact my local IT support or the Help Desk (4-HELP).

### If you interact with a computer, computer security is important to you.

Ensure that the integrity, confidentiality, and availability of data are maintained at an appropriate level all times. Computer security is an ongoing process, not a one-time effort.

Don't reinvent the wheel or stress on how to implement security controls. Capitalize on services provided to you by the University that will save your time, and that will very likely provide you with a higher level of security.

Where possible, engage your local IT support staffs about services, software, and resources that are available to you.

Take the time to review and follow IT policy, which governs all personal or unmanaged devices connecting to the campus network. Policy is developed to protect you and the University community from harm (such as loss, damage, or exposure of data), as well as to achieve compliance with federal and state regulations.

See [http://itsecurity.uiowa.edu/policy](http://itsecurity.uiowa.edu/policy) for a complete list of University IT policies.

---

END USER - Self Managed System/ Device Compliance

Why struggle for solutions when you can automate?