PROTECTING RED-HOT DATA

A GUIDE TO SAFE HANDLING OF CRITICAL INFORMATION

INDIANA UNIVERSITY
INFORMATION POLICY OFFICE
INFORMATION SECURITY OFFICE

What exactly is critical information?

Need-to-know information

Some information requires special care and handling, especially when inappropriate handling of the information could result in:

- Criminal or civil penalties
- Identity theft or personal financial loss
- Invasion of privacy, and/or
- Unauthorized access to this type of information by an individual or many individuals.

There are many different kinds of information that need special handling. For example, all personally identifiable student education records, including student grades, are sensitive and need reasonable levels of protection.

But some information is **RED HOT** and is classified by IU as "critical." Requiring the very highest level of protection, this critical information includes:

- Social Security numbers (SSN)
- Credit card numbers
- Debit card numbers
- Bank account or other financial account numbers
- Driver's license numbers
- State ID card numbers
- Student loan information
- Protected health information or individually identifiable health information relating to past, present, or future conditions, provisions of health care, and payment for the provisions of health care
- Foundation donor data
- Passport number
- International Visa number
- Passwords, passphrases, PIN numbers, security codes, and access codes. **Note:** Personal passphrases and codes should NEVER be shared with anyone.

Usually, a critical information element needs to be accompanied by an individual's name in order to result in harm due to inappropriate handling, but not always. If enough information is included to be able to identify someone, it may still be a red hot situation!

Check with the UIPO at uipo@iu.edu or 812-855-UIPO if you are unsure whether you need to apply special care and handling to the information elements and assets you use.

Collection and Retention

Need-to-Know Information

Collection

Whenever you are requesting or collecting critical information from a person or source, STOP and CONSIDER:

Why do I need this info? Is it REQUIRED for this situation? Can I fulfill my purpose without it?

- If you do not absolutely need it to transact that business, DISPOSE of it securely.
- If you received the information from another source, DIRECT THE SOURCE not to provide it to you anymore.

Can I make the information less sensitive, and still fulfill my business need?

- Collect the last four digits of SSNs instead of full number.
- Remove columns of critical info prior to making reports.
- Convert SSNs to university ID numbers for former students/staff.

If you must collect critical information...

- Inform your senior executive officer and ensure they approve of this use.
- Document the justification and approval to collect it.
- Notify the individual that you are collecting their data and explain its intended purpose.
- If appropriate, obtain the consent of the individual, preferably in writing.
- Consult with your departmental computing professional(s) and/or the appropriate data steward(s) to ensure you are handling it securely and appropriately.
- Destroy the information in a secure manner once you no longer require it.
- Regularly review your decision and your protection measures to ensure that the business need still exists and that the protection measures are still optimal.

Retention

The potential for unauthorized disclosures increases with the length of time information is retained. You should keep information, both electronic and paper, only as long as it is required for business needs. Federal and state law and university practice determine retention requirements. Consult with the office responsible for the information for current retention requirements, and monitor the University Records Management Schedules at www.libraries.iub.edu/index.php?pageId=3148

Storage of Sensitive Data

Need-to-Know Information

Securely dispose of all critical information, unless you absolutely cannot do business without storing your own copy.

Do you really need to store it?

Is it absolutely necessary to retain a copy locally? Or, does the university store the same information elsewhere? Try accessing and viewing the information from its primary university source, rather than creating another copy that will require special attention to protect.

Use SSH, VPN, or remote desktop to connect to the main storage location if you need access to critical information while mobile.

Use a SECURE storage location

All critical information in electronic format must be professionally secured. To prevent it from being compromised or stolen:

- ASK your department which server is professionally secured for critical information storage.
- NEVER store this information on your desktop workstation, laptop, PDA, USB drive, flash drive, or any mobile device/media unless (a) the information is properly encrypted on the device and (b) the senior executive officer of your unit or the Institutional Review Board has provided prior written approval confirming a critical business need for you to do so.
- NEVER store this information in personal storage areas, such as personal flash drives/discs, home computers, external email, or external online storage services.
- VERIFY that you're using a secured file server – many unauthorized exposures happen because files are placed on Web servers instead of FILE SERVERS.

Ensure paper records are kept in locked file cabinets/storage rooms or are otherwise access controlled. If you store paper records in University Archives, the IU Warehouse, or other shared locations, ensure that these records are not accessible to others storing records in the same location.

Safeguards

- Encrypt critical information if stored electronically.
- Always log off or lock your workstation when you step away, even for a moment.
- For more ways to safeguard critical information, see kb.iu.edu/data/akln.html

PROTECTING RED HOT DATA

Use & Transmission

Need-to-know information

Critical information is to be used only in conducting university business, and in ways consistent with furthering the university's mission.

- Never use information for personal gain or profit, the gain or profit of others, to satisfy curiosity, or to engage in academic, personal, or research misconduct.
- Use critical information only for the purpose for which it was collected.
- Report any misuse of information to the appropriate authorities. For more information, see: protect.iu.edu/cybersecurity/incident

Transmission by hand...

- Use reliable transport or couriers (the Purchasing Department maintains a list of authorized couriers).
- Verify the identity of couriers prior to providing info to them.
- Always require a signature from the recipient.
- Provide a full address for the recipient – not a P.O. Box.
- Keep your shipping documentation, including the tracking number.
- Follow up to ensure the information made it to the intended recipient.
- Protect information from unauthorized disclosure or modification during transit (for example, use locked containers or tamper-evident packaging).

Transmission electronically...

Encrypt while in transit from your sending location to the receiving location.

- If you cannot use an encrypted transit method, then encrypt the file itself, prior to sending it.
- Consider using Slashtmp: https://www.slashtmp.iu.edu
- Comply with HIPAA when transmitting health information
- Web sites must be coded securely and the information must be transmitted over a secure channel – see: kb.iu.edu/data/ahuq.html
- When using web sites for research purposes, the site must comply with HIPAA and/or CFR part 11 (for FDA related research).
- Learn about other methods of at: protect.iu.edu/cybersecurity/secure-file-transfer-alternatives

Help with Encryption

tools & resources

How does encryption help protect information?

Information stored or transmitted in an unencrypted form can be read by an attacker or thief very easily. When that same information is encrypted using a key, only the person who has access to the correct key will be able to decrypt the information.

The two methods of encryption

When you hear the word "encryption," it could apply to securing information in one of TWO situations:

1) While it is being stored, referred to as "**encrypting data at rest**"; and

2) While it is being transmitted, referred to as "**encrypting data in transit**."

There are different tools for each of these two uses.

If you must store and/or transmit critical information, you must use tools to encrypt the information. See the following resources, or consult with your computer support professional, to ensure you are encrypting information appropriately.

For information on encrypting **stored** critical information, see:

- protect.iu.edu/cybersecurity/data/encryption
- "What is PGP?" at: protect.iu.edu/tools/pgp
- "What is BitLocker?" at: kb.iu.edu/data/avjz.html
- "What is TrueCrypt?" at: kb.iu.edu/data/auhm.html

For information on encrypting **transmitted** critical information, see:

- Overview: protect.iu.edu/cybersecurity/secure-file-transfer-alternatives
- "What is SFTP?" | kb.iu.edu/data/akqg.html
- "What is IUVault?" | kb.iu.edu/data/asyf.html

Searching & Inventorying

Tools & Resources

Even if you think...

...you do not have any critical information anywhere under your control, you must take advantage of tools provided (such as Identity Finder) to help make sure.

Searching for critical information

Indiana University licenses Identity Finder, a tool that can search for, protect, and securely dispose of certain critical information elements stored on your computer, file shares, or external media. For more information, see:
protect.iu.edu/identityfinder

Identity Finder and similar tools also assist you in inventorying all locations that do contain critical information. You cannot protect critical information if you do not know you have it, so:

- Check to see if you have critical information on your departmental file server, your departmental/campus web servers, portable devices such as laptops or PDAs, and storage media (disks, USB keys, CDs, etc).
- Inform your departmental computing professional when you find critical information, and ask for assistance in disposing of or protecting it adequately.
- Identify where you have stored information on paper – including your desk or office area, file cabinets, closets, remote storage, and any other storage areas used by you or your unit.

About that Social Security number...

IU stopped using SSNs as employee IDs in December 2002, and student IDs in fall 2004. Therefore, it is important to review employee records prior to 2003, and student records prior to 2005, looking out for SSNs in particular. To purge those SSNs:

- Delete the SSN column and all the SSNs in it from historical student records.
- Look for colored papers (class rosters used to be printed on green or blue paper) or, for oversized sheets (about 10" by 13") of white paper (for records prior to 1989).
  - If not needed, shred!
  - If needed, ensure ones with SSNs are moved to secured storage.
- For external payrolls or government reporting, the university ID number can be converted to the SSN at the time of reporting.

Disposal, Wiping, & Shredding

Tools & Resources

Disposal

All critical information assets must be disposed of securely. Secure disposal means deleting information from media in a way that ensures the data is not recoverable. NEVER discard or leave any critical information in an area accessible to the public.

Deletion is not enough

Most methods of deleting a file from a computer's hard drive only remove pointers to the actual file – they do NOT remove the information itself. Most system utilities, and even ways to re-format the hard drive, do not remove the information either.

If you are still actively using the hard drive and are deleting small amounts of critical information (such as a column of SSNs in an old spreadsheet), it is OK to use normal deletion methods and then delete your deleted items. But if you are DISPOSING of a hard drive or any storage media, IU policy requires wiping or destroying them prior to disposal or transfer outside the university.

Disk wiping utilities

There are many utilities available for securely wiping a disk or other storage media prior to disposal. Check with your computing support professional for his or her preferred tool, or see:

- "How can I securely wipe disk drives using DBAN?" at: kb.iu.edu/data/auhn.html

Hard drive destruction

Destruction of the hard drive/storage media is often most effective. IU provides these data destruction services:

- IUB Surplus Data Destruction Service: iub.edu/~blpur/procedure/harddrive.shtml
- IUPUI Surplus Data Destruction Service: purchasing.iupui.edu/surplus_hardDrives.php
- Other IU campuses, use IUPUI Data Destruction Service.

For more information, see protect.iu.edu/cybersecurity/data/secure-removal

Shredding of paper

A list of approved document destruction vendors is available under "Document Destruction" at: www.iu.edu/~purchase/contract/contracts.html

PROTECTING RED HOT DATA

Sharing & Disclosure

Tools & Resources

Directly sharing with or providing any critical information elements to a person external to IU – verbally, on paper, or electronically – is a disclosure. Information may also be considered disclosed if a computer upon which information is stored is compromised or stolen; if information is made available via the Web; if paper records with the information are disposed of without shredding or the use of another secure disposal method; or if computer disks are disposed of without following one of the methods described here.

Authorized Disclosures

Sharing or disclosure of critical information is sometimes necessary, or even required by law, to complete a business transaction. Even so, be sure to evaluate and document it appropriately for authorization:

- Ensure that a recently reviewed contract (through IU Purchasing) is in place to oversee the sharing agreement.
  - Note: Contracts signed prior to 2006 must be updated to include new standard language.

- In many instances of sharing or disclosure, particularly when a SSN is included, you need to obtain the individual's express written consent. Documents should expressly indicate that the SSN is being disclosed.

- Any requests/demands from law enforcement or from the public under the Indiana Access to Public Records Act should be forwarded to the Office of the Vice President and General Counsel **IMMEDIATELY**.

Unauthorized Disclosures

If at any time you think you may have had an unauthorized disclosure or exposed any critical information, please **immediately**:

1) Call your Support Center or Network Operations Center
2) Send details to it-incident@iu.edu.

The Information Policy and Security Offices will be paged to coordinate a response. If the incident involves a possibly compromised computer, do not access or alter files/data, and do not power it off. Taking these actions will delete important forensic data. Instead, wait for instructions from the Policy and Security Offices.

Resources

Tools & Resources

University Information Policy Office
Phone: 812-855-UIPO
Web: protect.iu.edu/uipo
Email: uipo@iu.edu

Committee of Data Stewards
Web: datamgmt.iu.edu
Email: iudata@iu.edu

Information Protection Resources
Web:
protect.iu.edu/cybersecurity/data

Office of the VP and General Counsel
Phone: 812-855-9739
Phone: 317-274-7460

Student Privacy and FERPA
Web: registrar.indiana.edu/ferpainfo.shtml

IU Knowledge Base
Web: kb.iu.edu

Tips from IU on staying safe online
Web: protect.iu.edu/cybersecurity/safeonline

Support Center Contact Information
Web: kb.iu.edu/data/abxl.html (all campuses)

Network Operations Center
Phone: 317-274-7788

Institutional Data Acceptable Use Agreement
Web: protect.iu.edu/agreement