Critical Data Guide

A guide to handling critical information at Indiana University

Access the guide online at: *go.iu.edu/15Rz*

What exactly is critical information?

Certain information requires special care and handling, especially when inappropriate handling could result in:

- Criminal or civil penalties
- Identity theft or personal financial loss
- Invasion of privacy
- Unauthorized access to the information

Many kinds of information require special handling. For example, all personally identifiable student education records, including grades, are sensitive and require reasonable levels of protection.

But some information is especially sensitive 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 numbers
- International Visa numbers
- 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.

Check with the University Information Policy Office (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

Collection

Whenever you request or collect critical information from an individual or institutional source, stop and consider: Why do I need this information? Is it required for this situation? Can I fulfill my purpose without it?

- If you do not absolutely need it, dispose of it securely.
- If you received the information from another source, ask the source to avoid sharing it with you in the future.

Can you make the information less sensitive, and still fulfill your business need?

- Collect only the last four digits of SSNs instead of the complete nine-digit number.
- Convert SSNs to university ID numbers when possible and appropriate.
- Remove columns of critical and other individually identifiable info prior to creating reports.

If you must access or collect critical information...

- Inform your unit leader and ensure they approve of this use.
- Consult with your departmental IT Professional(s) (*kb.iu.edu/d/baxq*) and/or the appropriate data steward(s) (*datamgmt.iu.edu*) to ensure secure and appropriate handling.
- Document the justification and approval.
- Notify individuals that you are collecting their data and explain its intended purpose.
- If appropriate, obtain the consent of the individuals, preferably in writing.
- Determine if the information is subject to university policy, local, state, or federal laws. Consult with General Counsel if needed.
- Destroy the information in a secure manner once you no longer require it.
- Regularly review your decision and your protection measures to ensure the business need still exists and the protection measures are still optimal.

Retention

The potential for unauthorized disclosure increases with the length of time you retain information. Keep information, in any form, 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 (*go.iu.edu/15HF*).

Storage of sensitive data

Storage

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 on a user's individual computer or department server? Or, does the university maintain the same information elsewhere? Rather than creating another copy that will require special protections, access and view the information from its primary university source.

Use Secure Shell (SSH), virtual private network (VPN), remote desktop, or other methods using strong cryptography to connect to the main storage location.

Use a secure storage location

Not all storage locations are acceptable for critical information. Critical information in electronic format must be professionally secured to prevent it from being compromised or stolen:

- Ask your department which storage service is professionally secured for critical information storage.
- Never store this information on your desktop, laptop, mobile device, USB drive, flash drive, or any media unless (a) the information is properly encrypted and (b) the senior executive officer of your unit has provided prior written approval confirming a critical business need to do so. For more information, see the Mobile Device Security Standard IT-12.1 (*go.iu.edu/15HG*).

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 at rest if you store it electronically.
- Always log off or lock your workstation when you step away, even for a moment.
- For more ways to safeguard critical information see the article Best Practices for Computer Security (*kb.iu.edu/d/akln*).
- Some information, like payment card or health information, can have special requirements (e.g., PCI DSS and HIPAA).

For more PCI DSS information, see: *go.iu.edu/15HH*
For more HIPAA information, see: *go.iu.edu/15HI*

Use and transmission

Use and transmission

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

- Use critical information solely for the purpose for which it was collected.
- 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.
- Immediately report any misuse of information to the appropriate authorities. For more information, see: *go.iu.edu/15HJ*.

Transmission by hand

- Use reliable transport or couriers. See the Media Disposal Guide for a list of approved couriers: *go.iu.edu/15HK*
- Verify the identity of couriers prior to providing info to them.
- Protect information from unauthorized disclosure or modification during transit (for example, use locked containers or tamper-evident packaging).
- 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.

Transmission electronically

Encrypt while in transit.

- If you cannot use an encrypted transit method, then encrypt the file itself prior to sending. Consider using Slashtmp: *www.slashtmp.iu.edu*
- When transmitting health information or payment card information, comply with PCI DSS or HIPAA as appropriate.

For more PCI DSS information, see: *go.iu.edu/15HH*
For more HIPAA information, see: *go.iu.edu/15HI*

- Websites must be secure and transmit information over a secure channel. For more information, see: *go.iu.edu/15HL* and *kb.iu.edu/d/ahuq*
- When used for research purposes, websites may need to comply with HIPAA, CFR part 11 (for FDA related research), or the Federal Information Security Modernization Act (FISMA: *www.dhs.gov/fisma*).
- Learn about other methods of protecting data during electronic transmission at: *go.iu.edu/15HM*

Tools and resources

Encryption assistance

How does encryption protect information?

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

The two methods of encryption

Encryption secures information in one of two situations:

1. While it is being stored, referred to as "encrypting data at rest"
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 store and/or transmit critical information, you must encrypt the information.

See the following resources or consult with your IT Professional to ensure you are encrypting information appropriately.

For information on encrypting stored critical information, see:

- Overview: *go.iu.edu/15HN*
- "What is PGP?" at: *kb.iu.edu/d/azmy*
- "What is BitLocker?" at: *kb.iu.edu/d/avjz*

For information on encrypting transmitted critical information, see:

- Overview: *go.iu.edu/15HM*
- "What is SFTP?" at: *kb.iu.edu/data/akqg.html*
- "What is Slashtmp, and how do I use it?" at: *kb.iu.edu/data/angt.html*
- "About the Cisco Secure Email Encryption Service (CSEES)" at: *kb.iu.edu/d/bbtq*

Searches and inventories

Even if you think you do not have any critical information under your control, there are tools like Identify 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: *go.iu.edu/15HR*

Identity Finder and similar tools also assist with inventorying locations that 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, tablets, or smart phones; and storage media (disks, USB keys, CDs, etc).
- Inform your departmental IT Professional if you find critical information, and ask for assistance in disposing of or protecting it adequately.
- Identify where you have stored critical 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 (SSN)

IU ended the use of SSNs as employee IDs in 2002, and student IDs in 2004. Therefore, it is important to review employee records prior to 2003, and student records prior to 2005, looking for SSNs in particular.

To purge old records of 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 oversized sheets of white paper (about 10" X 13" — usually for records prior to 1989).
    - If you do not need them, shred them!
    - If you need them, ensure records with SSNs are moved to secured storage.
- For external payrolls or government reporting, a university ID number can be converted to a SSN at the time of reporting.

Disposal, wiping, and shredding

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 reformat 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 fine to use normal deletion methods and then delete your deleted items.

However, if you are disposing of a hard drive or any storage media, IU policy (*go.iu.edu/15HS*) requires wiping or destroying them prior to disposal or transfer outside the university.

Disk wiping utilities

Many utilities will securely wipe a disk or other storage media prior to disposal. Check with your computing support professional about preferred tools, or see:

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

Hard drive destruction

Destroying the hard drive/storage media is often most effective, and IU provides the IU Surplus Data Destruction Service:

- IU Bloomington: *go.iu.edu/15HT*
- IUPUI: *go.iu.edu/15HU*

For more information, see: *go.iu.edu/15HV*

Shredding paper

A list of approved document destruction vendors is available under "Document Destruction" at: *go.iu.edu/15HW*

The IU Warehouse also provides secure shredding services to Bloomington campus departments. See: *go.iu.edu/15RC*

Sharing and disclosure

Directly sharing or providing critical information elements to a person outside IU — verbally, on paper, or electronically — is a disclosure.

Information disclosure may also take place when:

- A computer upon which information is stored is compromised or stolen
- Information is made available online or via an external application
- Paper records with the information are disposed in an unsecure manner
- Computer media is disposed in an unsecure manner

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 the authorization appropriately:

- 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, particularly when a SSN is included, you need to obtain an individual's express written consent for sharing or disclosure. Documents should expressly indicate that their SSN is being disclosed.
- 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**.
- All disclosures must comply with Policy DM-02, Disclosing Institutional Information to Third Parties, which requires a University Information Security Office review and Data Steward approval for the disclosure of critical data. See: *go.iu.edu/15HX*

Unauthorized disclosures

If at any time you think critical information has been disclosed or exposed without authorization:

1. Immediately call the following in order — no matter what time of day or night (or weekday, weekend, or holiday) — until you reach someone:
   - UIPO/UISO: (812) 855-8476 (during normal business hours)
   - UITS Network Operations Center: (812) 855-3699 (24x7)
   - UITS Support Center: (812) 855-6789 (after hours)
2. Send details to: *it-incident@iu.edu*

The Information Policy and Security Offices will coordinate a response.

If the incident involves a possibly compromised computer, do not use the system. This means you should not do a network scan of the system, run antivirus software, patch the system, reboot, unplug any cables, or power off the system. Taking these actions will destroy important forensic data. Instead, wait for instructions from the Policy and Security Offices. For more information, see: *go.iu.edu/15HJ*

Key contacts

University Information Policy Office
(812) 855-UIPO
protect.iu.edu/about/
uipo@iu.edu

Committee of Data Stewards
datamgmt.iu.edu
iudata@iu.edu

Office of the VP and General Counsel
IU Bloomington: (812) 855-9739
IUPUI: (317) 274-7460
www.indiana.edu/~vpgc/

UITS Support Center
kb.iu.edu/data/abxl.html (all campuses)

Network Operations Center
(317) 274-7788

Key websites

Information Protection
go.iu.edu/15HY

Student Privacy and FERPA
go.iu.edu/15I1

Staying safe online
go.iu.edu/15HZ

Institutional Data Acceptable Use Agreement
go.iu.edu/15I0

IU Knowledge Base
kb.iu.edu

Critical Data Guide: A guide to handling critical information at Indiana University
Printed copies available upon request. Contact the University Information Policy Office: *uipo@iu.edu*