INDIANA UNIVERSITY (HTTP://WWW.IU.EDU)

Acceptable Use Agreement

Access to Institutional Data and Information Technology Resources

Introduction

You have been directed to this Acceptable Use Agreement as a result of your need for access to institutional data and information technology resources at Indiana University.

Access to Indiana University data and information, and access to IT accounts, systems, and applications, is based on your need for access and your assent to use that access appropriately. These services are integral to the operation of the university, and security and privacy laws and other institutional policies protect much of the information.

Therefore, before you can be granted access, you must read and agree to follow these acceptable usage standards, and must accept responsibility to preserve the security and confidentiality of information that you access, in any form, including oral, print, or electronic formats.

Read the information below carefully. It begins with an explanation of how data use is governed within IU, and then sets out user responsibilities. Although these general provisions apply when you use or access any IU information, IT accounts, systems, or applications, please be aware that managers of certain services or information types may require you to complete additional agreements and/or training.

Information Governance Explained

The university has assigned the following roles concerning data and information.

Data Ownership: Although individual units or departments may have stewardship responsibilities for portions of the institutional data, Indiana University is considered the data owner of all university institutional data.

Data Stewards: For the purposes of information security and privacy governance, Data Steward is a Role Title and is defined as an individual who has been named to represent information, usually for a specific information type, business sector, or business function, for university-wide information governance purposes. Data Stewards are responsible for establishing policies, procedures, and

guidelines for institutional data management across Indiana University. Individually, each Data Steward has management and policy-making responsibilities for their specific data subject areas and as part of the virtual institutional data base.

Data Managers: Data managers are assigned responsibilities to receive, evaluate, and authorize or deny requests for access to systems, applications, and/or databases containing institutional information in electronic or in paper form.

Information Classification Explained

Institutional data varies in its sensitivity to the university and must be handled in a way that is commensurate with its risk and criticality. Therefore, the university has defined 4 data classifications to assist users in determining the appropriate handling of institutional data.

Institutional Data (or information) is data in any form, location, or unit that meets one or more of the following criteria:

- It is subject to a legal obligation requiring the University to responsibly manage the data;
- It is substantive and relevant to the planning, managing, operating, documenting, staffing or auditing of one or more major administrative functions or multiple organizational units of the university;
- It is included in an official university report;
- It is clinical data or research data that meets the definition of "University Work" under the Intellectual Property Policy UA-05; or
- It is used to derive any data element that meets the above criteria.

Data Stewards apply the following criteria to classify institutional data and information into four levels:

- Public
- University-internal
- Restricted
- Critical

Public: Few restrictions; generally releasable to a member of the public upon request; upon receipt of a request, seek advice from the appropriate data steward; if the request is made pursuant to the Indiana open records statute, seek advice from the Office of the VP and General Counsel, as well as the appropriate data steward.

University-internal: May be accessed by eligible employees and designated appointees of the university in the conduct of university business.

Restricted: Because of legal, ethical, or other constraints, may not be accessed without specific authorization, or only selective access may be granted. (Typically, your eligibility to access this data will be based on your job responsibilities.)

Critical: Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals. (Typically, your eligibility to access this data will be based on your job responsibilities.)

Usage Responsibilities

The following points detail your responsibilities as you access, use, or handle information or information technology (IT) at IU.

Secure Usage

You agree to:

- **Never share your account password(s), passphrase(s) or multi-factor authentication devices with anyone including friends, roommates, family or IU staff.**
- Select strong password(s) and passphrase(s) and change them regularly.
- Never use your IU credentials for non-IU systems and applications.
- Be mindful that different computer systems and applications provide different levels of protection for information, and seek advice on supplemental security measures, if necessary. For example, a mobile laptop, tablet, or smartphone provides inherently less protection than a desktop computer in a locked office. Therefore, the level of protection provided to information accessed or stored using a laptop is to be supplemented by using additional safeguards such as encryption technology, enhancing physical security, restricting file permissions, etc.
- Respect the university's information and system security procedures (i.e., never attempt to circumvent or "go around" security processes).
- Make appropriate use of the tools provided (e.g., strong passphrase, virus/malware protection, encryption software, encrypted transmission, digital signatures, multi-factor authentication, training, etc.) to uphold the security of the university's IT systems and applications, and the confidentiality of information stored on them.
- Take steps to understand "phishing attacks," computer viruses, and other destructive software, and take steps to protect your accounts from such threats (e.g., never reply to emails asking for account

passwords or passphrases, never open unsolicited email attachments, never click unknown links, always verify the sender of emails asking for university-internal, restricted and/or critical data, use virus scanning software, apply system patches in a timely manner, etc.).

- Immediately notify the University Information Policy Office (it-incident@iu.edu) if you believe your account credentials (e.g., user ID, password, passphrase, multi-factor authentication device, etc.) have been compromised.
- Maintain information in a secure manner to prevent access, viewing, or printing by unauthorized individuals.
- Secure unattended computers (e.g., log off, lock, or otherwise make inaccessible), even if you will only be away from the computer for a moment.
- Store Restricted and Critical data securely (e.g., on secure servers, in locked file cabinets, in services certified for appropriate data classifications, etc.).
- Securely dispose of Restricted and Critical information (e.g., by shredding, disk wiping, physical destruction, etc.). See University Policy DM-01s: Standards for Management of Institutional Data for more information about the storage and disposal of Restricted and Critical data.
- Never copy and/or store Restricted or Critical data outside of institutional systems (e.g., on desktop workstations, laptops, USB drives, personally owned computers, etc.) without proper approval from the senior executive officer of the department and only in cases where it is absolutely necessary for the operation of the department.
- Take appropriate steps to secure information (e.g., password protection, encryption, etc.) on mobile devices (e.g., laptops, tablets, USB drives, smartphones, etc.) including verifying that all mobile devices used to work with institutional data are in compliance with the Mobile Device Security Standard IT-12.1 (https://protect.iu.edu/online-safety/policies/it121.html).
- Ensure, in the rare cases where Critical data has been approved for use and storage outside of institutional systems, that the data are appropriately encrypted, especially on mobile devices (e.g., laptops, tablets, smartphones, USB drives, CD-ROMs).
- Ensure, in the rare cases where it is necessary to email Critical data, that the data are sent to the correct recipient and only via encrypted email methods.

Legal Usage
You agree to:

- Use information and IT for legal purposes only.
- Respect and comply with all copyrights and license agreements.

- Never use your access to information or IT to harass, libel, or defame others.
- Never damage equipment, software, or data belonging to others.
- Never make unauthorized use of computer accounts, access codes, or devices.
- Never monitor or disrupt the communications of others, except where explicitly authorized by the University.
- Never use IT to view or distribute child pornography.
- Abide by applicable laws and policies with respect to access to, use, disclosure, and/or disposal of information.
- Report unauthorized access to, inadequate protection of, and inappropriate use, disclosure, and/or disposal of information, immediately to the University Information Policy Office (UIPO) via email: it-incident@iu.edu.

WARNING: Unauthorized distribution of copyrighted material using Indiana University's information technology resources -- including sharing copyrighted music, movies, and software through peer-to-peer applications like Limewire, BitTorrent, MP3Rocket, Frostwire, etc. using Internet access provided by IU -- is against the law and university policy. In addition to sanctions the university may impose, unlawful file sharing may subject you to legal penalties. This includes both civil penalties (having to pay money to the copyright holder in a lawsuit) and criminal penalties (fines and jail time). For additional information, see: https://protect.iu.edu/online-safety/personal-preparedness/file-sharing/index.html.

Ethical Usage
You agree to:

- Access institutional information only in the conduct of university business and in ways consistent with furthering the university's mission of education, research, and public service.
- Use only the information needed to perform assigned or authorized university duties.
- Never access any institutional information to satisfy your personal curiosity.
- Use information and IT in ways that foster the high ethical standards of the university.
- Never use information or IT to engage in academic, personal, or research misconduct.
- Never access or use institutional information (including public directory information) for your own personal gain or profit, or the personal gain or profit of others, without appropriate authorization.
- Respect the confidentiality and privacy of individuals whose records you may access.

- Preserve and protect the confidentiality of all University-internal, Restricted, or Critical information as a matter of ongoing responsibility.
- Never disclose University-internal, Restricted, or Critical data (as defined by policy; see above) or distribute such data to a third party in any medium (including oral, paper, or electronic) without proper approval, and in the case of Restricted or Critical data, without a contract processed through or waived by the IU Purchasing Department.

Facilitative Usage
You agree to:

- Never cause community or shared resources to be inaccessible or unusable.
- Use shared information technology resources efficiently.
- Regularly delete unneeded files and information from your accounts (if not required to retain them as outlined in university policy or records management schedules).
- Avoid overuse of network bandwidth, information storage space, printing facilities, paper, processing capacity, or other shared information technology resources.
- Never send mass email (i.e. unsolicited bulk email or spam) without appropriate approval.
- Never send or respond to chain email.

Policies and Laws

You should be aware that institutional policies, federal and state laws, international laws and contractual obligations exist that provide further protections to certain types of information, or that may influence how you handle information. Data Managers of certain applications and information types may require you to complete additional training to familiarize you with these.

Examples of relevant IU policies include the following:

- IT-01: Appropriate Use of IT Resources (http://policies.iu.edu/policies/categories/information-it/it/IT-01.shtml): Establishes appropriate usage requirements.
- IT-07: Privacy of Electronic Information and IT Resources (http://policies.iu.edu/policies/categories/information-it/it/IT-07.shtml): Establishes the procedures and circumstances under which an individual's electronic accounts and files may be accessed by others.
- IT-11: Excessive Use of Information Technology Resources (http://policies.iu.edu/policies/categories/information-it/it/IT-11.shtml): Establishes limitations on

excessive use of IT resources.

- IT-12: Security of IT Resources (http://policies.iu.edu/policies/categories/information-it/it/IT-12.shtml): Establishes appropriate security requirements.
- IT-12.1: Mobile Security Standard (https://protect.iu.edu/online-safety/policies/it121.html): Establishes minimum security requirements for mobile devices.
- ISPP-26: Information and Information System Incident Reporting, Management, and Breach Notification (http://policies.iu.edu/policies/categories/information-it/ispp/ISPP-26.shtml)
- DM-01: Management of Institutional Data (http://policies.iu.edu/policies/categories/information-it/data-management/DM-01.shtml)
- DM-01-S: Standards for Management of Institutional Data (http://policies.iu.edu/policies/categories/information-it/data-management/DM01s.docx)
- *For a more comprehensive list, see:* http://policies.iu.edu/policies/categories/information-it/index.shtml (http://policies.iu.edu/policies/categories/information-it/index.shtml)

Examples of relevant federal laws include:

- **Family Educational Rights and Privacy Act (FERPA)** Provides students rights of access to their education records and generally prohibits the disclosure of student education records without the prior written consent of the student.
- **Health Insurance Portability and Accountability Act (HIPAA)** Imposes various privacy and security requirements on personal health information collected or maintained by certain units of the university.
- **Financial Services Modernization Act of 1999 ("Gramm Leach Bliley") and accompanying FTC Standards for Safeguarding Customer Information** Requires universities to develop and implement an information security program designed to protect nonpublic personal information gathered and maintained with respect to certain financial activities, most commonly student financial aid activities, other lending activities, and check-cashing activities.
- **The Fourth Amendment to the US Constitution, and various federal and state laws concerning access by law enforcement to information** Establishes the procedures and circumstances under which law enforcement authorities may gain access to institutional data. All warrants, subpoenas, and other legal requests, demands, or orders seeking access to institutional data or systems must be forwarded immediately to the IU Office of the Vice President and General Counsel.

Examples of relevant state laws include:

- **State of Indiana Access to Public Records Act** With some exceptions, provides for public access to government records, including records of public universities like IU. All requests for records under the Indiana Access to Public Records Act must be forwarded immediately to the IU Office of the Vice President and General Counsel.
- **Indiana Code 4-1-10** With some exceptions, makes it a crime to disclose more than the last four digits of someone's Social Security number to someone outside of the university.
- **Indiana Code 4-1-11** With some exceptions, requires that the university promptly notify individuals when a breach of electronic systems security reasonably appears to have resulted in unauthorized access to individuals' unencrypted personal information, including Social Security numbers, credit and debit card numbers, driver's license numbers, and financial account numbers or access codes.
- **Indiana Code 24-4-14** With some exceptions, requires that the university securely dispose of records with unencrypted personal information in them including Social Security numbers, credit card numbers, driver's license numbers, and financial account numbers or debit card numbers in combination with security or access codes or passwords.
- **State invasion of privacy laws** Generally prohibit the disclosure of personal information about an individual when doing so would be highly offensive to a reasonable person.
- **State libel/defamation laws** Generally prohibit false statements that harm another's reputation.

An example of a relevant contractual obligation includes the following:

- **Payment Card Industry Data Security Standards (PCI-DSS)** A contractual obligation when accepting credit cards for payment (or contracting for others to do so on IU's behalf), it requires strict security safeguards be applied to protect credit card numbers and associated data from unauthorized access. At IU, the Treasury Department oversees all credit card processing activities.

Sanctions

Indiana University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances involved this could include the offices of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the General Counsel, and/or appropriate law enforcement agencies. See policy IT-02, Misuse and Abuse of Information Technology Resources (http://policies.iu.edu/policies/categories/information-it/it/IT-02.shtml) for more detail.

Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

Assent

To be entrusted with access to Indiana University data and information, IT accounts, systems, and applications, you must accept these responsibilities and standards of acceptable use. By accepting these terms, you agree to follow these rules in all of your interactions with IU data, information, and information technology.

If you choose not to accept these standards of conduct, you may be denied access to information and/or information technology.

The terms of this agreement may change periodically. The most current version can always be found at the following URL: https://access.iu.edu/UserAgreement/SignAgreement.

By entering "YES" as your e-signature into the box below, you hereby accept the terms and conditions of this agreement. You have read, understand, and agree to abide by the terms and conditions of this agreement.

Please type "YES" in the box as your e-signature:

Submit

FULFILLING *the* PROMISE

INDIANA UNIVERSITY