Technology Usage Best Practices

2014

Indiana State University Foundation

Office of Advancement Services

Effective May 1st, 2014

Last Updated May 1st, 2014

Contents

Introduction

Philosophy on Technology Usage

The Technology Usage Best Practices document covers all technology used by Foundation users in performing their jobs including, for example, personal computers, mobile phones, online services, and tablets. It does not attempt to cover all situations or answer every question regarding technology usage. Rather, we trust our users to use common sense and informed best judgment in making decisions in the best interest of the Foundation. This document contains information and guidelines intended to enable you to use technology to maximize productivity and effectiveness while also protecting the Foundation, its reputation, and its information assets.

The Foundation maintains an active information security program to ensure that reasonable safeguards are in place to protect the Foundation and its information. However, our philosophy is to balance information security with stewardship of resources and flexibility of technology usage. This means that every person working on behalf of the Foundation has a responsibility toward securing information assets.

You are empowered to use technology to maximize your productivity with few restrictions. In return, your obligation is to make informed and educated decisions regarding the technology that you use so as not to expose the Foundation to undue risk. If you encounter a situation that is not addressed, or if you simply have questions regarding this document, please contact the Foundation's Database and Technology Services.

Information Security

Confidentiality

The successful operation and the reputation of the Foundation are built upon the principles of fair dealing and ethical conduct by our directors and employees. The Foundation's reputation for integrity and excellence requires careful observance of the spirit and the letter of all applicable laws and regulations, as well as a scrupulous regard for high standards of conduct and personal integrity.

The continued success of the Foundation is dependent upon our stakeholders' and donors' trust. The Foundation is dedicated to preserving that trust. Directors and employees have an obligation to the Foundation, its donors, and its other stakeholders to act in a way that will merit their continued trust and confidence and the trust and confidence of the general public.

All data and information that comes through the Foundation offices or is located in the Foundation database or on its servers is confidential. Information is not to be shared with others, including other offices of the University that do not have privileges to it and others outside of the Foundation and University, including family and friends. A violation can result in an immediate dismissal and further action may be taken based on the severity of the infraction.

If a situation arises where it is difficult to determine what the proper course of action should be. The matter should be discussed openly with the employee's immediate supervisor and, if necessary, the Chairman of the Foundation's Audit Committee for advice and consultation.

Compliance with the Confidentiality Policy is the responsibility of each Foundation employee and those University employees who have access to the above mentioned Foundation information. Disregarding or failing to comply with this policy will result in sanctions ranging from a written warning to termination of employment. Necessary sanctions will be determined and enforced by the appropriate Associate Vice President, Vice President, President or the Foundation Board of Directors.

Foundation-Issued Equipment

Foundation-issued equipment is for staff (that is, Foundation employees and contingent workers) use only. Depending on your role at the Foundation, you will be assigned Foundation-issued equipment to use in performing your job. You are responsible both for the equipment issued and its use. Always exercise caution if leaving your equipment unattended.

User Credentials

Depending on your role at the Foundation, you will be assigned credentials that grant you the access necessary to do your job. These credentials are for your use only, and you are responsible for their safekeeping. Your credentials provide access to your confidential personal information, such as HR data, as well as confidential Foundation data. For these reasons, you must never share your password with anyone. Do not reuse your Foundation passwords on external web sites or applications. If the external site is compromised, the Foundation could be at unnecessary risk. Please contact Database and Technology Services immediately if you believe your credentials may have been compromised. Refer to the Password Management Policy for best practices on creating and managing secure passwords.

Computer Safeguards

Foundation-issued equipment has been configured with a number of safeguards to assist you in having a secure computing experience. These safety mechanisms may include, but are not limited to, antivirus software, screen locks, firewalls, automatic software patching, and encryption. It is essential for the security of the Foundation that these safety mechanisms remain enabled and functional as configured. Contact Database and Technology Services as soon as possible if one of these safeguards is not functioning properly.

Appropriate Storage Locations

Any information that could cause significant financial or reputational harm should be stored only in an approved manner on appropriate foundation-issued equipment and systems. The Foundation has designated internal network storage locations as approved storage locations for Foundation data. Hard drives, outside of approved network storage, and other media such as laptop or external hard drives, USB flash drives, and CD/DVDs, are not appropriate storage locations for Foundation data beyond occasional and very short-term use. These devices are typically not enabled with the same safeguards as Foundation-issued devices and may be easily lost or compromised.

You are responsible for complying with the Foundation's policies for ensuring that Foundation information is appropriately protected. More information about the storage and retention of Foundation data may be found in the records management policies and the Email Policy. The foundation is under no obligation to maintain, retain, back up, or return any data located on a temporary storage device (such as laptop or external hard drives, USB flash drives, or CD/DVDs). Any

data stored on laptop hard drives may be removed at the Foundation's sole discretion and without prior notification.

In no event may any user delete or destroy data that may be relevant to a pending or threatened claim or government investigation. For more information, refer to the records management policies.

Information Management

As with the technology devices themselves, you are expected to use informed good judgment when handling Foundation information. Exercise care when sending or receiving confidential information outside of the Foundation. Email and online sharing services (such as YouSendIt and DropBox) may not be sufficiently secure depending on the sensitivity of the information. When sending information outside of the Foundation, please adhere to the records management policies and use appropriate storage locations.

Employees are not allowed to:

- Violate copyright laws by downloading, installing or using unlicensed software or by transmitting copyrighted materials belonging to entities other than the Foundation. Failure to observe copyright or license agreements may result in disciplinary action from the Foundation or legal action by a copyright owner;
- Hack or attempt to hack into other networks including: attempting to gain access to restricted resources inside or outside the Foundation's network;
- Use the internet in such a way that it disrupts the operation of the Foundations network or the networks of other users;
- Share personnel files on the internet; and
- Use the internet or technology systems to send messages with derogatory or inflammatory remarks about an individual's or group's age, disability, gender, race, religion, national origin, physical attributes, sexual preference or any other classification protected by federal, state or local law.

Non-Foundation Devices

Generally, you are expected to use Foundation-issued equipment for conducting Foundation business. Do not connect non-foundation devices (that is, devices not provided and managed by Foundation IT) to the Foundation's internal network. This helps ensure the safety and security of the Foundation's network and information assets.

Non-Foundation Personnel

In some cases, when appropriate, the Foundation may grant access to its technology and data systems to non-Foundation personnel. As with Foundation personnel, non-personnel will be required to adhere to the confidentiality agreement.

Awareness of Surroundings

In order to prevent the inadvertent disclosure of confidential or sensitive information, consider your surroundings when you engage in discussions or work on sensitive documents. Be particularly careful in airports, restaurants, and other public venues. Note that rooms containing camera or audio equipment

may not be secure. Where available, in-room controls may be used to ensure cameras or audio equipment are disabled when not required.

Monitoring of Electronic Content, Electronic Communications, and Systems Use

It is not the Foundation's regular practice to monitor electronic content, electronic communications, or system use. However, the Foundation reserves the right to perform such monitoring as it deems necessary. Monitoring may be performed without notification to support activities such as, but not limited to, operational maintenance, auditing, and security.

Information Stewardship

Stewardship at the Foundation applies not only to money and donors, but to the use and security of technology and information. In keeping with the Foundation's guiding principles you are expected to consider stewardship in your decisions regarding technology and information resources.

Personal Use of Foundation Technology Resources

The Foundation recognizes the importance of allowing occasional and limited personal use of Foundation technology. In the case of certain classes of devices (such as mobile phones), alternate guidance may be provided regarding personal use. You are ultimately responsible for any and all activity that originates from your use of Foundation technology. The Foundation takes no steps to maintain, retain, back-up, or return personal data. As Foundation systems are subject to monitoring, you should not store sensitive or confidential personal information on Foundation resources. Such permitted personal use does not include individual political activities, which should occur during off-duty hours, at the employee's expense and without use of the Foundation's name, resources, facilities, or equipment.

Access to all areas of the internet is allowed from within the Foundation; however, the Foundation reserves the right to control access to any non-business related internet service, if necessary, to control bandwidth. Efforts will be made to provide access to all internet services; however, non-business related internet services may be blocked, possibly without notice, if necessary.

Physical Loss

When transporting Foundation-owned equipment, please be aware of your surroundings. Although the Foundation has taken steps to prevent data from being misappropriated or misused in the event of lost or stolen equipment, you should treat Foundation-issued equipment as if it were your own. The Foundation does not back up data stored on mobile equipment. If you believe any of your Foundation-issued equipment has been lost or stolen, contact Database and Technology Services immediately.

Software and Technology Services Not Provided by IT

The freedom to install software and use external technology services is a significant privilege and therefore carries significant responsibility. Unpatched software is a common source of viruses, worms, and other malware, which pose a threat to the Foundation's information assets. Software written by untrustworthy authors can result in loss of confidential data or system compromise. Use of online services can result in unintended disclosure of Foundation information assets.

If you install software on a Foundation-issued device or use external technology services, you must understand the associated risks (such as the trustworthiness of the author, download source, impact to information security, and system performance and reliability). You are responsible for managing these

risks, including ensuring that the software or service is properly licensed and kept current with security patches. If the software has an auto-update function, consider enabling it. Procurement of software and technology services must be in accordance with the Foundation's policies regarding purchasing.

If you have any concerns or questions, contact Database and Technology Services for advice, or do not install the software. For Windows and other officially supported applications, the Foundation Database and Technology Services will provide regular updates.

Blogging and Social Networking

Employees who maintain personal blogs (i.e. web sites that contain online personal journals with the writer's reflections and comments including Facebook, Twitter, LinkedIn, and other similar social networking interfaces) or who post messages on the blogs of others are legally responsible for anything they post. This includes blogging about the Foundation, its business, employees, and students. Employees who blog should think carefully before blogging about the Foundation and should avoid comments that violate Foundation policies, including the Policy Against Sexual Harassment and Other Workplace Harassment, or that are false, malicious, obscene, or that might reveal confidential, proprietary, or trade secret information.

Legal

You are expected to use technology resources in accordance with all applicable laws and Foundation policies.

Licensing and Copyright Laws

When installing or using software not provided by the Foundation, you must ensure that the software is properly licensed. This also applies to copyrighted materials including music, videos, and movie files, as well as written media.

Electronic Content and Messaging

The Foundation's e-mail, telephone, voicemail, fax, internet and technology systems belong to the Foundation, and the Foundation reserves the right to monitor and examine all communications over these systems at its discretion. Accordingly, no employee should have any expectation of privacy as to his or her internet or technology systems usage and should not use these systems for information they wish to keep private. These systems should be used primarily for Foundation-related business. Personal use of e-mail, voicemail, fax and the internet is acceptable, but should be done using good judgment and with the recognition that these systems are provided in order to conduct business. Federal and State law and Foundation policies regarding intellectual property, misuse of Foundation property, discrimination, harassment, sexual harassment, information and data security and confidentiality apply to the use of all Foundation technology systems.

Recordings of Video, Web, or Telephone Conferences

Before recording any meeting or telephone conference, organizers should determine whether recording the meeting session is appropriate. Further, to comply with privacy laws, the organizer must inform all presenters and participants that the recording is taking place prior to the start of the meeting by providing the following statement:

IMPORTANT NOTICE: This meeting is being recorded by the Foundation. Any documents and other materials exchanged or viewed during the meeting session may also be recorded. By joining this meeting, you consent to such recording. If you do not consent to the recording, you have the option not to participate in the meeting.

Appendices

Confidentiality Statement

ISU Foundation Employee Handbook

The successful operation and the reputation of the Indiana State University Foundation are built upon the principles of fair dealing and ethical conduct by our employees and volunteers. The Foundation's reputation for integrity and excellence requires careful observance of the spirit and the letter of all applicable laws and regulations, as well as a scrupulous regard for high standards of conduct and personal integrity.

The continued success of the Foundation is dependent upon our stakeholders' and donors' trust. The Foundation is dedicated to preserving that trust. Foundation and university employees, along with volunteers have an obligation to the Foundation, its donors, and its other stakeholders to act in a way that will merit their continued trust and confidence and the trust and confidence of the general public.

All data and information that comes through the Foundation offices or is located on the Foundation database is confidential. Information is not to be shared with others, including other offices of the University that do not have privileges to it and others outside of the Foundation and University, including family and friends. A violation can result in an immediate loss of rights to information and further action may be taken based on the severity of the infraction.

If a situation arises, where it is difficult to determine the proper course of action, the matter should be discussed openly with the departments leadership in which you are receiving the information and, if necessary, the Chairman of the Foundation's Audit Committee for advice and consultation.

Compliance with this confidentiality document is the responsibility of each Indiana State University Foundation employee, volunteer, and those University employees who have access to the above mentioned Foundation information. Disregarding or failing to comply with these will result in sanctions ranging from a written warning to termination of duties associated with the Foundation. Necessary sanctions will be determined and enforced by the appropriate Vice President, President or the Foundation Board Executive Council.

I, _____, have read the above statements and agree to comply with them to the best of my ability. I acknowledge the policies that I must follow related to the use of the information that comes through the Foundation or is found within the Indiana State University Foundation database. I understand that any breach of the policies could result in various sanctions, including immediate termination.

_____ _____

(Name) ***(Date)***

Email Policy

1. Purpose
The purpose of this policy is to ensure the proper use of Indiana State University Foundation's email system and make the users (defined below) aware of what the Indiana State University Foundation deems as acceptable and unacceptable use of its email system. This policy also provides for sanctions in cases of breach of violation of the policy terms.

2. Applicability
This policy applies to the use of the Indiana State University Foundations email services by the users at the Indiana State University Foundations offices, as well as remote locations, including, but not limited to, the users homes, airports, hotels, and client offices.
All Indiana State University Foundation employees, including full-time or part-time, independent contractors, interns, consultants, guests, board members, clients, University employees and other third parties who have been granted the right to use the Indiana State University Foundation's email services are defined as the users for the purpose of this policy and are required to sign this agreement confirming their understanding and acceptance of this policy.

3. Email Accounts are the Property of the Indiana State University Foundation
All email accounts maintained on the Indiana State University Foundation's email systems are property of the Indiana State University Foundation. Indiana State University Foundation has the right to read and keep a record of any emails that users transmit via the Indiana State University Foundation's email system. The Indiana State University Foundation reserves the right to monitor all email transmitted via the Indiana State University Foundation's email system. Employees have no reasonable expectation of privacy when it comes to business and personal use of the Indiana State University Foundations email system.

4. Email exists for Business Purposes only
The Indiana State University Foundation allows its email access primarily for business purposes. The users may use the Indiana State University Foundation's email system for personal use only in accordance with this policy.

5. Authorized Personal Email Use
Although the Indiana State University Foundations email system is meant only for business use, the Indiana State University Foundation allows the reasonable use of email for personal use subject to the following guidelines:
Personal emails must also adhere to the guidelines in this policy.

6. Unacceptable Use of Email
The following acts shall constitute unacceptable use of the email system of the Indiana State University Foundation:
Use of the Indiana State University Foundations communications systems to send chain letters;
Forwarding of the Indiana State University Foundations confidential messages or information to external locations;

Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal;
Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment;
Accessing copyrighted information in a way that violates the copyright;
Breaking into the Indiana State University Foundations or another organizations system or unauthorized use of a password/mailbox;
Broadcasting unsolicited personal views on social, political, religious or other non-business related matters;
Using email to operate another business, conduct an external job search, or solicit money for personal gain;
Transmitting unsolicited commercial or advertising material outside of the Indiana State University Mission;
Undertaking deliberate activities that waste staff effort or networked resources;
Introducing any form of computer virus or malware into the corporate network as seen fit by Indiana State University Foundation;

7. Legal Risks Involved
Email is a business communication tool and the users are obliged to use this tool in a responsible, effective, and lawful manner. Although by its nature email seems to be less formal than other written communication, similar laws apply. Therefore, it is important that users are aware of the following legal risks of email. Both the user and the Indiana State University Foundation can be held liable for:
a. sending emails with any libelous, defamatory, offensive, racist or obscene remarks;
b. forwarding emails with any libelous, defamatory, offensive, racist or obscene remarks;
c. unlawfully forwarding confidential information of others or to others;
d. copyright infringement for unlawfully forwarding or copying messages without permission purposely or deliberately
e. sending an attachment that contains a threat.
The above list does not enumerate all the legal risks involved however, by following the guidelines provided in this policy; the users can minimize the legal risks involved in the use of email. If any user disregards the rules set out in this Email Policy, Indiana State University Foundation can take corrective action up to and including termination of employment.

8. Business Record Retention Policy email messages are written business records and are subject to the Indiana State University Foundations rules and policies relating to retaining and deleting business records.

9. Confidential Information
Avoid sending confidential information by email. Unless authorized to do so, the users are prohibited from using email to transmit confidential information to outside parties.
Confidential information includes, but is not limited to:
a. client lists;
b. credit card numbers;
c. Social Security numbers;
d. employee performance reviews;
e. salary details;

f. passwords; and
g. any other information that could embarrass or disgrace the Indiana State University Foundation and its associates if the information were disclosed to the public.

10. Disclaimer
The following disclaimer shall be added to each outgoing email:
This electronic mail message, including attachments, is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any unauthorized use, review, disclosure, distribution, or actions taken in reliance on the contents of this information, is prohibited. If you received this email in error and are not the intended recipient, please notify me immediately by telephone or reply email and destroy all copies of the original message. The recipient should check this email and any attachments for the presence of viruses. The Indiana State University Foundation accepts no liability for any damage caused by any virus transmitted by this email.

11. Violations and Sanctions
If an employee is found to violate any of these email policy rules, the Indiana State University Foundation could take disciplinary action up to and including termination of employment and potential legal action.
The actual penalty applied will depend on factors such as the seriousness of the breach, the employee's disciplinary record, and any other factors the Indiana State University Foundation deems necessary to consider.

12. Amendment of Policy
The Indiana State University Foundation reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

13. Questions
If you have any questions or comments about this Email Policy, please contact Suzi Zurcher, by phone at 812-249-4207 or email at szurcher@indstatefoundation.org. If you do not have any questions, the Indiana State University Foundation presumes that you understand and are aware of the rules and guidelines in this email policy and will adhere to them.

14. Declaration
I have read, understand, and acknowledge receipt of the email policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary action up to termination of employment and potential legal action.

_____ _____

Password Management Policy

Passwords

Network passwords have the following parameters in place:

- Minimum length of 7 characters
- Complex: require at least one upper case letter, lower case letter, number or symbol (special character)
- Expire every 90 days
- Previous 24 passwords are saved and cannot be repeated
- After 5 unsuccessful logon attempts, the account is locked out for 30 minutes

RE/FE passwords have the following parameters in place:

- Minimum length of 8 characters
- Require at least one upper case letter, one lower case letter, and one number or special character
- Users can change their own password
- If account is locked out, user must wait 30 minutes to retry

While there are no specifications on passwords expiring within RE or FE, all users must have a Beyond Nines Remote desktop connection.

Remote Access Standards

All staff users in the organization can remotely access their email either through web or outlook anywhere, via username/password, secured by a verisign certificate. The Foundation has VPN access to the site for administration.

Within the Foundation five departments have outside VPN access. For these users VPN access is no different than being in the building and is subject to the same restrictions.

Authorization for VPN permissions go through the Director of Database and Technology or Associate Vice President of Advancement Services. Installation of VPN access is given to Gibson Teladata to install or remove. The firewall records when a user accesses VPN, for how long, and if they tried to access something they should not.

Software Applications

Software permissions are granted at time of hire for new employee's based on limited accessibility for assigned permission for that position. Permission are granted or denied as necessary for the required job functions. Permissions are granted through the Director of Database or Technology and the Associate Vice President of Advancement Service.

All other software applications use secure user name and password identification process to access information through a secure web portal.

The following are general recommendations for creating a Strong Password:

A Strong Password **should** -

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~!@#$%^&*()_-+=)

A Strong Password **should not** -

- Spell a word or series of words that can be found in a standard dictionary
- Spell a word with a number added to the beginning and the end
- Be based on any personal information such as user id, family name, pet, birthday, etc.

The following are several recommendations for maintaining a Strong Password:

- **Do not share your password with anyone for any reason**
  Passwords should not be shared with anyone, including any students, faculty or staff. In situations where someone requires access to another individual's protected resources, delegation of permission options should be explored. Passwords should not be shared even for the purpose of computer repair. An alternative to doing this is to create a new account with an appropriate level of access for the repair person.

- **Change your password periodically**
  As a general rule of thumb, changing your password every 90 days is recommended. However, you may choose to vary the frequency of password changes based on the privilege or access level of the account. Accounts of greater privilege or access level should have their password changed more frequently and vice versa. This practice prevents someone, who has obtained your password through some means, from continuing to have access to your account. If you suspect someone has compromised your account, change your password immediately and contact Technology and Database Services.

- **Consider using a passphrase instead of a password**
  A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters inserted throughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional benefits such as being longer and easier to remember. For example, the passphrase "My passw0rd is $uper str0ng!" is 28 characters long and includes alphabetic, numeric and special characters. It is also relatively easy to remember. It is important to note the placement of numeric and symbolic characters in this example as they prevent multiple words from being found in a standard dictionary. The use of blank spaces also makes a password more difficult to guess.

- **Do not write your password down or store it in an insecure manner**
  As a general rule, you should avoid writing down your password. In cases where it is necessary to write down a password, that password should be stored in a secure location and properly destroyed when no longer needed. Using a password manager to store your passwords is not recommended unless the password manager leverages strong encryption and requires authentication prior to use.

- **Avoid reusing a password**
  When changing an account password, you should avoid reusing a previous password. If a user account was previously compromised, either knowingly or unknowingly, reusing a password could allow that user account to, once again, become compromised. Similarly, if a password was shared for some reason, reusing that password could allow someone unauthorized access to your account.

- **Avoid using the same password for multiple accounts**
  While using the same password for multiple accounts makes it easier to remember your passwords, it can also have a chain effect allowing an attacker to gain unauthorized access to multiple systems. This is particularly important when dealing with more sensitive accounts such as your Andrew account or your online banking account. These passwords should differ from the password you use for instant messaging, webmail and other web-based accounts.

- **Do not use automatic logon functionality**
  Using automatic logon functionality negates much of the value of using a password. If a malicious user is able to gain physical access to a system that has automatic logon configured, he or she will be able to take control of the system and access potentially sensitive information.

The following are Guidelines for individuals responsible for provisioning and support of user accounts:

- **Enforce strong passwords**
  Many systems and applications include functionality that prevents a user from setting a password that does not meet certain criteria. Functionality such as this should be leveraged to ensure only Strong Passwords are being set.

- **Require periodic password changes**
  Forcing a periodic password change serves as a reminder to users and eliminates the human factor in determining whether to change a password. A general rule of thumb is to force a password change every 90 days.

- **Require a change of initial or "first-time" passwords**
  Forcing a user to change their initial password helps ensure that only that user knows his or her password. Depending on what process is being used to create and distribute the password to the user, this practice can also help mitigate the risk of the initial password being guessed or intercepted during transmission to the user. This guidance also applies to situations where a password must be manually reset.

- **Force expiration of initial or "first-time" passwords**
  In certain situations, a user may be issued a new account and not access that account for a period of time. As mentioned previously, initial passwords have a higher risk of being guessed or intercepted depending on what process is being used to create and distribute passwords. Forcing an initial password to expire after a period of time (e.g. 72 hours) helps mitigate this risk. This may also be a sign that the account is not necessary.

- **Do not use Restricted data for initial or "first-time" passwords**
  The Guidelines for Data Classification defines Restricted data in its data classification scheme. Restricted data includes, but is not limited to, social security number, name, date of birth, etc. This type of data should not be used wholly or in part to formulate an initial password. See Appendix A for a more comprehensive list of data types.

- **Always verify a user's identity before resetting a password**
  A user's identity should always be validated prior to resetting a password. If the request is in-person, photo identification is a sufficient means of doing this. If the request is by phone, validating an identity is much more difficult. One method of doing this is to have the user fax in a copy of their photo id. However, this can be a cumbersome process. Another option is to have the person's manager call and confirm the request. For obvious reasons, this would not work for student requests. If available, a self-service password reset solution that prompts a user with a series of customized questions is an effective approach to addressing password resets.

- **Never ask for a user's password**
  As stated above, individual user account passwords should not be shared or any reason. A natural correlation to this guidance is to never ask others for their passwords. Once again, delegation of permission is one alternative to asking a user for their password. Some applications include functionality that allows an administrator to impersonate another user, without entering that user's password, while still tying actions back to the administrator's user account. This is also an acceptable alternative. In computer repair situations, requesting that a user create a temporarily account on their system is one alternative.

The following are several additional Guidelines for individuals responsible for the design and implementation of systems and applications:

- **Change default account passwords**
  Default accounts are often the source of unauthorized access by a malicious user. When possible, they should be disabled completely. If the account cannot be disabled, the default passwords should be changed immediately upon installation and configuration of the system or application.

- **Implement strict controls for system-level and shared service account passwords**
  Shared service accounts typically provide an elevated level of access to a system. System-level accounts, such as root and Administrator, provide complete control over a system. This makes these types of accounts highly susceptible to malicious activity. As a result, a more lengthy and complex password should be implemented. System-level and shared service accounts are typically critical to the operation of a system or application. Because of this, these passwords are often known by more than one administrator. Passwords should be changed anytime someone with knowledge of the password changes job responsibilities or terminates employment. Use of accounts such as root and Administrator should also be limited as much as possible. Alternatives should be explored such as using sudo in place of root and creating unique accounts for Windows administration instead of using default accounts.

- **Do not use the same password for multiple administrator accounts**
  Using the same password for multiple accounts can simplify administration of systems and applications. However, this practice can also have a chain effect allowing an attacker to break into multiple systems as a result of compromising a single account password.

- **Do not allow passwords to be transmitted in plain-text**
  Passwords transmitted in plain-text can be easily intercepted by someone with malicious intent. Protocols such as FTP, HTTP, SMTP and Telnet all natively transmit data (including your password) in plain-text. Secure alternatives include transmitting passwords via an encrypted tunnel (e.g. IPSec, SSH or SSL), using a one-way hash or implementing a ticket based authentication scheme such as Kerberos.

- **Implement automated notification of a password change or reset**
  When a password is changed or reset, an email should be automatically sent to the owner of that user account. This provides a user with a confirmation that the change or reset was successful and also alerts a user if his or her password to unknowingly changed or reset.

Approved by the ISU Foundation Board of Directors – July 2013

Record Retention & Destruction Policy

Record Retention & Destruction Policy

Purpose

In accordance with best practices of the Sarbanes-Oxley Act, which makes it a crime to alter, cover up, falsify, or destroy any document with the intent of impeding or obstructing any official proceeding, this policy provides for the systematic review, retention, and destruction of documents and records received by or created by the Indiana State University Foundation (Foundation) and/or its subsidiaries in connection with Foundation business. This policy covers all records and documents, regardless of medium of storage, and contains guidelines for how long certain documents are retained. The policy is designed to ensure compliance with federal and state retention policy, laws and regulations, to eliminate accidental or innocent destruction of records, and to facilitate the Foundation operations by promoting efficiency and freeing up valuable storage space.

Definition

A record is defined as any information or data that is received by or made by Foundation staff in the course of their duties. The record can be generated in multiple mediums including, but not limited to handwritten or typed form, e-mail, electronic documents including scanned originals and scanned archival materials, tapes, film, microfilm, photocopies, microfiche, flash drives, optical disks, and computer disks.

Ownership

All documents are the property of the Foundation and may not be removed, destroyed, mutilated, transferred, or otherwise damaged or disposed of, in whole or in part, except as provided by this policy. Outgoing board members and staff may not remove any records from the Foundation.

Document Storage/Oversight

Documents may be stored within the Foundation offices, in University archives, in a long-term storage facility, or retained and electronically archived on a secure server. The oversight of record storage and access will be the responsibility of the Chief Financial Officer who will assure that backups are in place for disaster recovery, that only appropriate staff has access to records and that security is in place for the destruction of records.

Each respective area within the Foundation is responsible for workflow design and image processing for electronic record storage. Records should not be maintained in both paper and as electronic records

with limited exceptions. These exceptions include active signed vendor contracts, real estate transactions, endowment agreements, and auditable records.

Retention Schedule

Where appropriate regulations exist, records will be maintained according to rulings as set forth by the Internal Revenue Service.

Records that are critical including those which may substantially affect the obligations of the Foundation or that may be pertinent to any ongoing or anticipated government investigation, proceeding or private litigation will not be destroyed.

Other records will be retained as follows:

Type of Document	Retention Time
Accounting and Finance	
Accounts payable ledgers and schedules	7 years
Audit reports	Permanently
Bank Reconciliations	3 years
Bank statements	3 years
Depreciation Schedules	Permanently
Duplicate deposit slips	3 years
Expense Analyses/expense report forms	7 years
Year End Financial Statements	Permanently
Financial statements (end-of-year)	Permanently
General ledgers and end-of-year statements	Permanently
Investment performance reports	Permanent
Paid Invoices (to customers, from vendors)	7 years
Inventories of products, materials, and supplies	7 years
Corporate Documents and Contracts	
Articles of Incorporation	Permanently
Contracts, mortgages, notes and leases (expired)	7 years
Contracts (still in effect)	Permanently
Deeds, mortgages, and bills of sale	Permanently
Insurance Policies (expired)	3 years
Board of Directors and committee meeting minutes; subsidiary boards' meeting minutes	Permanently
Minute books, bylaws and charter	Permanently
Patents and related Papers	Permanently
Trademark registrations and copyrights	Permanently
Correspondence: Legal and Donor	
Correspondence (general)	3 years
Correspondence (legal, tax, and other important matters)	Permanently
Correspondence (with donors or heirs/if deemed to have historical importance)	Permanently
Correspondence (with customers and vendors)	3 years
Donor Records	

Donation records of endowment funds and of significant restricted funds	Permanently
Donation records, other	10 years
Donor Agreements (Endowment Gifts)	Permanently
Donor Agreements (Current Use Gifts)	7 years after last disbursement
Human Relations Documentation	
Employment applications	3 years
Insurance records, current accident reports, claims, policies, etc.	Permanently
Payroll records and summaries	7 years
Personnel files (terminated employees)	7 years
Retirement and pension records	Permanently
Tax returns and worksheets	Permanently
Timesheets	7 years
Withholding tax statements	7 years

Approved by the ISU Foundation Board of Directors – July 2013

Corporate Records Management Policy

Corporate Records Management Policy

Purpose

The corporate records of the Indiana State University Foundation (Foundation) are assets. Accordingly, these assets require safeguarding to insure the existence of corporate records, completeness of business transactions, control of valuable information, the ability to locate records for the purposes of contract compliance and auditing, the ability to interpret business transactions and for fiscal transparency. The efficiency and integrity of the records management policy requires training for all staff to understand the need and structure of the filing system, commitment of management to assure the policy is adhered to and accountability of the staff charged with logging, filing and retrieving corporate records.

Definition

A corporate record is any document received by or created by the Foundation that meets at least one of the following criteria:

1) Establishes our existence as a 501(c)(3) entity
2) Protects, safeguards and assures our not-for-profit status is maintained
3) Reduces potential and inherent liability and risk
4) Establishes a contractual relationship related to the general business of the Foundation
5) Supports the acquisition of real property
6) Pertains to legal matters of the general business of the Foundation

Ownership

All corporate records are the property of the Foundation and may not be removed, destroyed, mutilated, transferred, or otherwise damaged or disposed of, in whole or in part, except as provided by the Record Retention and Destruction Policy or Internal Revenue Service rulings. Outgoing board members and staff may not remove any corporate records from the Foundation

Document Storage/Oversight

Corporate records may be stored within the Foundation offices in the general corporation filing system, in University archives, in a long-term storage facility or retained and electronically archived on a secure server. The oversight of corporate records will be the responsibility of the Chief Financial Officer (CFO) who will assure that backups are in place for disaster recovery, that only appropriate staff has access to corporate records and that security is in place for the destruction of corporate records.

Corporate Records Lifecycle

All corporate records are managed according to which stage of the records lifecycle they are in. Various internal controls are in place to assure the integrity of the document remains of utmost concern. The stages of the corporate records lifecycle:

1) Creation

a. Gift, pledge and endowment agreements follow approved templates and are reviewed by the Vice President of Development for compliance prior to signature
b. Contracts with vendors and providers are reviewed by the CFO for compliance prior to signature
c. Agreements are official when signed by Board designated authorities
d. Fulfillment of contractual activities, i.e., payments to vendors or establishment of funds, will not occur until corporate records are complete

2) Integration
   a. Immediately following signature or receipt, corporate records are delivered to Financial Services for dissemination to gift processing and accounts payable as needed
   b. Funds and vendors are established within the Raisers Edge and Financial Edge
   c. Corporate records are scanned and filed
3) Compliance
   a. Original corporate records must be checked out to remove them from the filing system and are expected to be returned within 10 business days
   b. The CFO will audit the corporate records system on an annual and intermittent basis to assure that records are being appropriately maintained
4) Archive
   a. Annually, the filing system will be reviewed for movement of records to permanent storage or destruction in accordance with the Records Retention Policy
   b. All destruction of corporate records will be logged on the destruction list

Filing Structure

Corporate records are stored by entity and category with alphabetical headers within each category. Various subcategories may exist within each category depending on file volume and differentiation of records needs.

*the following is not all-inclusive and will be updated once the structure is in place

Entity	Category	Header
Indiana State University Foundation, Inc.	Incorporation	Articles of Incorporation
		Bylaws
		501 (c)(3) Determination
	Audit	Annual Audit
		Correspondence
		Engagement Agreement
		Management Letter
	Board and Committees	Roster
	Accounting	Legal Interpretations
		Management Estimates
	Agreements	Gift Agreements
		Endowment Agreements
		Pledge Agreements
	Annual Reports	Business Entity Report
		Certificate of Good Standing

	Banking	Account Information
		Correspondence
	Insurance	FY13 Policy
		FY12 Policy
		FY11 Policy
	Investments	FEG Agreement
		FEG Reports
		FEG Correspondence
	Legal	Correspondence
	Memberships	CASE
		Country Club of Terre Haute
	Real Property	Buzash
		Munsee
	Rental Agreements	22 N. 5th St. LLC
		WestOhio LLC
	Property Tax Exemption	FY13 Filings
		FY12 Filings
		FY11 Filings
	Vendor Contracts	Art Spaces
		Blackbaud
		Gibson Teledata
Sycamore Foundation Holdings, Inc.	Incorporation	Articles of Incorporation
		Bylaws
		501 (c)(3) Determination
	Board	Roster
	Accounting	Legal Interpretations
		Management Estimates
	Agreements	Agreements
	Annual Reports	Business Entity Report
		Certificate of Good Standing
	Banking	Account Information
		Correspondence
	Insurance	FY13 Policy
		FY12 Policy
		FY11 Policy
	Legal	Correspondence
	Real Property	Riverfront
	Rental Agreements	Indiana State University
		Global Tower
		One Source
	Partnerships	22 N. 5th St. LLC
	Property Tax Exemption	FY13 Filings
		FY12 Filings
		FY11 Filings

	Terre Haute Rex Baseball	Accident Reports
		Franchise Agreement
		Sponsorship Agreements
		Vendor Agreements