1. Determine How Much Protection your Information Needs

The amount/type of protection to be applied to your information depends on an assessment of the need for the ***Confidentiality*** and/or critical nature of that information. The table below summarizes this process. For more detail regarding what types of information require Category I, II, or III Protection, refer to the Data Classification and Handling Policy, and Appendix 1: Data Classification Categories I, II and III.

How would you describe your information?

Is it ***Confidential***?	**Category I Protection**	**STOP! SPECIAL CARE IS REQUIRED**
Is there a ***high need*** for ***Integrity***?		
Is there a ***high need*** for ***Availability***?		
Is it ***Sensitive***?	**Category II Protection**	**BE VERY CAUTIOUS**
Is there a ***medium need*** for ***Integrity***?		
Is there a ***medium need*** for ***Availability***?		
Is it ***Public***?	**Category III Protection**	**PROCEED WITH AWARENESS**
Is there a ***low need*** for ***Integrity***?		
Is there a ***low need*** for ***Availability***?		

The rest of this Guide is organized so that you can see what protections are required or recommended for your information, based on the classification category you have determined.

2. Collect Only What is Necessary

	Category I	**Category II**	**Category III**
A. Collect only the minimum required amount of data to fulfill institutional responsibilities.	Required	Required	Required
B. Collect Social Security Numbers only as required to achieve necessary institutional purpose.	Required	Not Applicable	Not Applicable
C. Retain full credit card numbers (electronically or on paper), only if written approval has been obtained from the Comptroller's Office, the E-commerce committee, and the IT Security Office. *See Internet-based Credit Card Processing Policy for more information on handling this type of Confidential Information.*	Required	Not Applicable	Not Applicable

3. Provide Minimum Necessary Access

	Category I	Category II	Category III
A. Limit access to information to those with a legitimate interest (“need to know” or “need to do”) based on their institutional responsibilities.	Required	Required	Required
B. Access or attempt to access only information required to fulfill your institutional responsibilities.	Required	Required	Required
C. DO NOT log in for other people who are trying to access the computer system, e-mail system or other device. Never use anyone else’s login information.	Required	Required	Required
D. Grant access only to those authorized by the data owner.	Required	Required	Recommended
E. Use an authentication process to control access to non-public file systems. - Authentication means individuals attempting to gain access must have been previously approved for access and must prove their identity for each requested access by entering their user name and password or using another approved method of identification.	Required	Required	Not Applicable
F. Ensure all vendor access has been approved by the IT Security Office.	Required	Required	Required
G. Track and review who has gained access by recording ALL access in a system log. At a minimum, successful and failed login events, successful and failed account management events, and successful and failed policy and system events should be logged. (The logs should be stored in a way that precludes system administrators from altering/deleting them. The logs will be reviewed for anomalies monthly.)	Required	Recommended	Recommended
H. Information must be protected from unintended access by unauthorized users. - Guard against unauthorized viewing of such information displayed on your computer screen, keyboard, or login screen. - Do not leave information unattended and accessible. - Do not leave keys or access badges for rooms or file cabinets containing information in areas accessible to unauthorized personnel. - When printing, photocopying or faxing information, ensure that only authorized personnel will be able	Required	Required	Recommended

to see the output. If these machines retain the last document or several documents in memory, be sure to clear the memory after sensitive documents have been processed. Use a fax cover sheet with a confidentiality statement.			
I. Respect the confidentiality and privacy of individuals whose records are accessed by observing ethical restrictions that apply to the information accessed and by abiding by all applicable laws and policies with respect to accessing, using, or disclosing information. At a minimum: - Ensure Confidentiality Agreements are signed by staff with access to those systems storing and/or processing Sensitive Information. - Use an approved login banner on services that support it in order to inform users of their rights and responsibilities.	Required	Required	Required
J. Revoke or modify access rights and privileges to information for any individual with new or different responsibilities. - This may include obtaining keys, deactivating user accounts, changing the category of network access, changing codes for key punch systems, or deactivating passwords used to obtain access. - To revoke or modify access rights to electronic mail or shared electronic resources, see IT's Accounts page.	Required	Required	Not Applicable
K. Establish a periodic review (at a minimum quarterly) of user accounts including the related access rights and privileges for employees in your unit and modify those rights when appropriate. - Maintaining a current list of employees and their corresponding access rights is one way to facilitate the review process.	Required	Required	Not Applicable
L. Restrict servers to a single primary function.	Required	Recommended	Recommended
M. Disable or remove unused services, applications, ports, and user accounts.	Required	Recommended	Recommended
N. Physically secure access to operating systems, servers, and network equipment by placing them in areas that allow access to be restricted.	Required	Required	Recommended

O. Secure portable devices and portable media devices when unattended (e.g., laptop, PDA, smartphone, etc., and CD's, DVD's, floppy disks, USB/Flash/Thumb drives, etc.).	Required	Required	Recommended
P. Secure backup media from unauthorized physical access.	Required	Required	Recommended
Q. Ensure system setup is done in an environment that is only accessible to authorized administrators.	Required	Required	Recommended
R. All systems shall use only the below KU-approved network and system login banner: "Access to electronic resources at the University of Kansas is restricted to employees, students, or individuals authorized by the University or its affiliates. Use of this system is subject to all policies and procedures set forth by the University in the Policy Library. Unauthorized use is prohibited and may result in administrative or legal action. The University may monitor the use of this system for purposes related to security management, system operations, and intellectual property compliance."	Required	Required	Recommended

4. Disclose Only the Minimum Necessary Information

	Category I	**Category II**	**Category III**
A. Do not discuss or display information in an environment where it may be viewed or overheard by unauthorized individuals.	Required	Required	Recommended
B. Limit a disclosure to the amount of information reasonably necessary to achieve the purpose of the disclosure.	Required	Required	Required
C. Disclose information only when necessary and only to the extent that such disclosure is consistent with University policy and permitted or required by law.	Required	Required	Recommended
D. Ensure the Office of the General Counsel reviews all subpoenas, search warrants, or other court orders prior to release of information.	Required	Required	Required
E. Refer requests for information from media representatives (i.e., reporters, TV news crews, etc.) to the Office of University Relations.	Required	Required	Required
F. Report immediately any potential or suspected breach or compromise of, or unauthorized / unexplained access to University information (electronic or paper) to the Information Technology Customer Service Center (785-864-8080).	Required	Required	Required

◻ The Information Technology Customer Service Center will notify the KU Privacy Officer and/or the KU IT Security Officer as required by the particular incident.			

5. Safeguard Information in Transit

	Category I	**Category II**	**Category III**
A. Use secure methods of transmission when sending any Private, Confidential, or Sensitive data. ◻ Secure methods include, but are not limited to: • Encryption (i.e., at least Triple DES or AES; use AES-256 when possible), • Virtual private network (VPN), • Secure HTTP (HTTPS – TLS required) • Secure FTP (SFTP), • Encrypted and password protected CDs separated from passwords (phoned in) and/or the decryption keys (hand carried), • Facsimile transmission to secure faxes, etc.	Required	Required	Recommended
B. Encrypt email when sending Private, Confidential, or Sensitive information, even to other authorized users. The encryption method and key storage method must be approved by IT Security. ◻ Examples of information that should not be sent by email (unless encrypted) include, but are not limited to: • Student lists, • Data subject to the Health Insurance Portability and Accountability Act (HIPAA), • Data subject to the Gramm-Leach Bliley Act (GLBA), or ◻ Use a confidentiality statement at the beginning or end of e-mails to notify the recipient of confidential content.	Required	Required	Recommended
C. Send faxes only when the intended recipient is present. ◻ Use a confidentiality statement at the beginning or end of e-mails to notify the recipient of confidential content. ◻ Verify fax numbers prior to transmission.	Required	Required	Recommended

D. Ensure information (including device(s) containing information) is physically secure at all times when carrying or hand-delivering it to a new location.	Required	Required	Recommended
E. Remove information from secure locations only with prior approval.	Required	Required	Recommended
F. Access information remotely using only secure methods approved by the KU IT Security Office. For example, KU Anywhere is a virtual private network that can be used to access Private Information remotely.	Required	Required	Recommended
G. Accessing or transferring Private Information (Confidential or Sensitive information) using on-campus wireless connections is NEVER appropriate, unless the wireless network is encrypted and it has been approved by the KU IT Security Office.	Required	Required	Not Applicable
H. Accessing and transporting Social Security Numbers via a portable device is NOT appropriate.	Required	Not Applicable	Not Applicable

6. Secure Physical Equipment and Resources

	Category I	**Category II**	**Category III**
A. Actively “lock” your workstation when you are away from your desk; do not just wait for the screen saver feature to self-activate.	Required	Strongly Recommended	Strongly Recommended
B. Use “strong” passwords that are not easily guessed. Ensure that computer monitors are situated in a manner that login screens cannot be observed by passersby. Any passwords written down should be securely stored. Detailed requirements in regards to password strength and password changes can be found in the KU Password Policy.	Required	Required	Required
C. Place devices that can be used to print information in secure locations.	Required	Required	Recommended
D. Use a variety of methods to help prevent information compromise. Use a properly configured and currently patched firewall. Actively monitor systems using Anti-virus software that is updated daily. Actively monitor systems using Anti-spyware that is updated daily.	Required	Required	Required

◦ Obtain automatic security updates, and implement them expediently. ◦ Click “No” if your web browser offers to save passwords. Alternatively, turn off the password saving feature in the browser. ◦ Be aware of the risks to privacy of information when using desktop search features like Google Desktop Search.			
E. Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, thumb drive, or laptop. ◦ Select portable device models that provide security options to protect information stored on the drive. ◦ For example, Personal Data Assistants (PDAs) may be set to require a password when turned on or are inactive for a few minutes. ◦ Enable pass-codes and inactivity timers on mobile devices that support them. ◦ Employ whole disk encryption on mobile devices including laptops, tablets, and smartphones. Enroll encrypted laptops in the IT Security Office central management system for encrypted devices.	Required	Required	Recommended
F. When evaluating new software or appliances, request a security review of the proposed items by the IT Security Office BEFORE purchasing or installing. ◦ The request to ITSO should be in writing, signed by the purchasing authority, prior to final selection of vendors or products.	Required	Strongly Recommended	Strongly Recommended
G. When making a change to a service, system, or business process, consider whether any currently functioning security measures will be disrupted. All changes or modifications to the standard architecture shall be documented along with any justifications.	Required	Required	Recommended
H. Conduct regular system backups. Backups help ensure the availability of data necessary to fulfill University responsibilities in the case of device failure, disaster or theft.	Required	Strongly Recommended	Strongly Recommended

◻ Restoration from backup should be regularly verified. ◻ Security logs in addition to primary data should be backed up. ◻ Backup files should be stored at a secure location sufficiently apart from the primary data source/storage so as not to be impacted by an event that might render the original data unusable.			
I. Immediately contact the local area public safety department if there is a theft of any computer, electronic storage media, portable or personal device containing or that has been used to process University information. ◻ Also alert the department responsible for the device. ◻ If you suspect any Private Information was on the stolen device, contact the Information Technology Customer Service Center (785-864-8080). The Information Technology Customer Service Center will notify the KU Privacy Officer and/or the KU IT Security Officer as required by the particular incident.	Required	Required	Required

7. Safeguard Information in Storage

	Category I	**Category II**	**Category III**
A. Employ physical protection for all devices (electronic and non-electronic) used to store data. ◻ Limit physical access, including the ability of the public to inadvertently view the data (i.e., as passersby). ◻ Filing cabinets & drawers, offices, labs, and suite doors containing data must be locked. Do not leave data on unattended desk tops or leave file drawers unattended and unlocked. ◻ When not in use, all easily transportable devices should be secured (e.g., in locked cabinets or drawers). ◻ Users of laptop and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling or working away from the University.	Required	Required	Recommended

◻ Electronic media used to store Confidential Information must be secured by password-protected encryption. The encryption method and key strength category must be approved by IT Security. ◻ Encrypt Confidential Information stored on any mobile device (laptop, tablet, smartphone, etc.) or other portable media device (CD's, DVD's, thumb drives, etc.) and utilize available security features on the device. Encrypted laptops should be enrolled in the IT Security Office's centralized management for encrypted devices.			
B. Store Confidential or Sensitive Information in a separate location when possible.	Required	Required	Not Applicable
C. Always encrypt Confidential and Sensitive Information prior to storage. Encrypting data helps ensure that if an access control is bypassed, the information is still not readily available. A standard and published encryption standard should be used. The encryption method and key strength category must be approved by IT Security. ◻ Encrypt media stored off-site or have a documented process to prevent unauthorized access.	Required	Required	Recommended
D. Securely store information. ◻ Limit custody/access to as few people as possible to enhance accountability. ◻ Document transfers of custody.	Required	Required	Recommended
E. Store data on systems that support access control (as described in Section 3 of this policy).	Required	Required	Recommended
F. Retain Social Security numbers only when required (by a "business-related" purpose) and ONLY in an encrypted file or truncated to last 4 digits. ◻ The following identification mechanisms should also be handled and protected with care: 1. KU Student ID numbers, 2. KU Employee ID numbers, 3. State of Kansas Employee ID numbers, and 4. the KU Online ID.	Required	Not Applicable	Not Applicable
G. Store credit card numbers (electronically or on paper) ONLY with written approval from the Comptroller's Office, the E-commerce committee, and the IT Security Office. ◻ Retain credit card information only long enough to process the transaction. ◻ See Internet-based Credit Card Processing Policy and the Payment Card Industry Data Security Standard for	Required	Not Applicable	Not Applicable

more information on handling this type of Confidential Information. For Point-of-Sale terminals, ensure that any printed reports show no more than the last four digits of the account number.			

8. Dispose of Information Securely When No Longer Needed

	Category I	Category II	Category III
A. When retention requirements have been met, records must be either immediately destroyed or placed in secure locations as described in this section for controlled destruction. No records that are currently involved in, or have open investigations or audits, or records for which a litigation "hold" has been issued, shall be destroyed or otherwise discarded.	Required	Required	Required
B. Review, purge and shred printed documents regularly (in accordance with published destruction schedules). Shred documents prior to disposal/recycling. Adequately secure any documents that must be stored temporarily prior to shredding so they are not accessible to anyone without authorization.	Required	Required	Not Applicable
C. Ensure complete destruction of information on electronic storage media, computers, and portable devices prior to disposal/recycling. Refer to the Electronic Data Disposal Policy and Procedure. Securely erase media prior to transfer to another individual or department. Securely erase data used for testing once testing is complete.	Required	Required	Not Applicable

9. Stay Informed About Information Risks

	Category I	Category II	Category III
A. Ensure completion of information awareness training provided by the University. All employees must complete security awareness training hosted in the talent management system at https://mytalent.ku.edu prior to accessing confidential information.	Required	Required	Required