| | | | | | |
|---|---|---|---|---|---|
| **DATE POLICY REQUEST TO PET:** | [INSERT PET MEETING] | | | | |
| **IS THIS A NEW POLICY OR CHANGE TO AN EXISTING POLICY?** | | **NEW** | **X** | **EXISTING** | |
| **CURRENT POLICY TITLE:** | 19.20 / Data Sensitivity Classification | | | | |

[redacted]

| | |
|---|---|
| | IDP IT – Chris Synder |
| | Media Resource Center – John Jones |
| | Faculty Senate – Jolynn Dowling (shared) [PENDING] |
| | Staff Senate – Kennedy rogers (shared) [PENDING] |
| | University Deans (shared) [PENDING] |
| | Human Resources – Vicki Whisenhant and HR leadership (shared) [PENDING] |

**HR**

c) Course descriptions;

d) Semester course schedules; or

e) Press releases and

c) Data regarded as a “trade secret” as defined by the Kansas Uniform

2. **Level of Protection.** Data with the highest risk requires the greatest level of protection to prevent compromise, whereas data with lower risk requires proportionately less protection. University Data may fall within multiple classification schemes. For instance, research data and non-sensitive PII could span across all four classifications. The level of protection required for research data and non-sensitive PII is dependent upon the entities who create, store, process or transfer it and the contractual agreements, laws, or regulations that govern those entities.

3. **Departmental Policies.** A University department, division, or unit that operates and is responsible for its own information technology system is required to follow the security safeguards required by University Information Security, unless University Information Security has expressly approved department-specific written security safeguards that address the safeguards for University Data within that department. Any department-specific security safeguards must comply with this policy.

4. **Contracts with Third Parties.** Contracts between the University and third parties involving University Data must include language requiring compliance with all applicable laws, regulations, and University policies related to data and information security. If University Data is used or disclosed in any manner other than allowed by the contract the University General Counsel office must be notified immediately.

**DEFINITIONS**

A. For the purpose of this policy only, the following definitions shall apply:

1. **Biometric Identifier.** Data generated from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that

technology. Genetic information does not include information about the sex or age of any individual.

11. **Least Privilege**: Means individuals, processes, and systems should only have the minimum level of access and permissions necessary to perform their legitimate functions.

12. **Need to Know**: Means individuals should only have access to data that is relevant and necessary for their academic, administrative, or research activities.

13. **Non-Controlled Affiliated Organizations**: Wichita State University Foundation and Alumni Engagement.

14. **Personally Identifiable Information (PII):** Any information relating to an identified or identifiable natural person, which is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

15. **Proprietary Data:** Information that is developed, created, discovered or otherwise owned by an individual or entity that must be maintained in a confidential manner if required by such individual or entity.

16. **Protected Health Information (PHI):** Individually identifiable health information that is created, received, or maintained by a Covered Entity, which is transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium (including paper records, photos, or images).

17. **Sensitive Personally Identifiable Information (SPII):** Personally Identifiable Information that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

18. **University:** Wichita State University and Controlled Affiliated Organizations.

19. **University Data:** All information or data, including University-owned Proprietary Data, that is created, stored, or processed in any format by the University or is transferred to or through the University including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

## QUESTIONS AND DEVIATIONS

A. Questions or concerns regarding this policy or data classification deviations may be submitted to Information Security by emailing askinfosec@wichita.edu or by calling (316) 978-4732.

## IMPLEMENTATION TIMELINE AND LEGACY DATA

A. All new information technology systems designed and implemented after December 31, 2026, must comply with all security safeguards required by University Information Security.

B. Data Owners and Data Custodians must have a written compliance plan for all existing information technology systems and legacy data by January 1, 2028. This plan shall address the data classification strategy and estimated resourcing requirements. This does not require all data to be classified for compliance. Plans may be reviewed by University Information Security or delegated department based upon institutional risk and need.

## APPLICABLE LAWS AND ADDITIONAL RESOURCES

A. Family Educational Rights and Privacy Act of 1974 (20 U.S.C. § 1232g; 34 CFR Part 99)

B.

E. NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Federal Information Systems and Organizations

F. NIST Special Publication 800-60, Vol. 1, Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories

G. Controlled Unclassified Information (CUI) Markings | National Archives and Records Administration

H. Kansas Open Records Act, K.S.A. § 45-215, *et. seq*.

A. Kansas Health Information Technology Act, K.S.A. § 65-6821, *et seq*.

B. K.S.A. § 21-6107: Crimes involving violations of personal rights

C. State of Kansas ITEC Policy 8010A: Kansas Data Compliance Requirements

D. State of Kansas ITEC Policy 7230A: Information Technology Security Standardshttps://gdpr-info.eu/

E. WSU Policy 3.12 / Security and Confidentiality of Student Records and Files

F. WSU Policy 9.21 / Compliance with Federal Export Regulations

G. WSU Policy 13.14 / Security of Payment Card Data

H. WSU Policy 19.18 / Third Party Data Transfers

I. WSU Policy 19.10 / Retirement of Computing and Information Technology Resources

J. WSU Policy 20.17 / Protected Health Information