WSU POLICY APPROVAL COVER PAGE

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				
REVISED POLICY TITLE:	N/A				
LAST REVISED DATE OF POLICY:	N/A				
INITIATING AUTHORITY:	Information Security and Chief Data Officer				

SUMMARY OF POLICY OR POLICY CHANGE:

The State of Kansas requires that all State agencies classify data based upon the sensitivity of the information. This policy provides the criteria and classification levels for all University data. This is also a federal requirement for protecting information under NIST 800-171/CMMC for NIAR, in addition to providing protections to the University.

REASON OR NEED FOR POLICY / SUMMARY OF CHANGES MADE TO EXISTING POLICY:

This policy has been created to ensure compliance with state and federal requirements for data classification and protection and to address audit findings related thereto.

APPLICABLE LAWS OR REGULATORY OR POLICY AUTHORITY:

ITEC Policy 8010A: Kansas Data Compliance Requirements

ITEC Policy 7230A: Information Technology Security Standards

NIST Special Publication 800-171

OTHER RELEVANT WSU POLICIES:

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

WSU Policy 9.21 / Compliance with Federal Export Regulations

WSU Policy 9.18 / Third Party Data Transfers

WSU Policy 20.17 / Protected Health Information

THE FOLLOWING UNIVERSITY STAKEHOLDERS WERE INCLUDED IN THE REVIEW AND APPROVAL OF THIS POLICY DRAFT / REVISION:

	Office of the General Counsel – Stacia Boden and Misha Jacob-Warren
	Information Security – Mark Rodee
	Information Security – Gina Riggs
	Information Technology – Ken Harmon
	Chief Data Officer – David Wright

	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]
OTHER NOTES FOR CONSIDERATION:	
N/A	
OWNER OF POLICY REQUEST FOR QUESTIONS:	David Wright

19.20 / DATA SENSITIVITY CLASSIFICATION

I. INITIATING AUTHORITY

A. Information Security and the Chief Data Officer serve as the initiating authority for this policy.

II. PURPOSE

A. Data and information are important assets of the University and must be protected from loss of integrity, confidentiality, and availability. The purpose of this policy is to set forth the requirements for classifying and protecting the University's Data in compliance with state and federal laws, regulations, and policies.

III. POLICY

A. **Data Sensitivity Classification.** All University Data must be classified in accordance with the requirements of this policy. The appropriate classification for a collection of University Data will be based on the most sensitive information within the collection, even if the collection contains other information that would fall within a less sensitive classification if it were stored separately.

B. **Data Owner Responsibility.** Data Owners are responsible for ensuring the proper classification and protection of all University Data that is under their control in accordance with University policy and all security safeguards required by University Information Security.

C. **Classification Schema.** The classification of University Data will be based on how the data is used, its sensitivity to unauthorized disclosure, and any requirements imposed by external agencies or applicable laws. All University Data, except for Classified National Security Information and third-party owned Proprietary Data, must be classified under the following four levels of data sensitivity classification:

1. **WSU Public Data.** WSU Public Data generally has a very low sensitivity, but it still warrants protection since the integrity and protection of the data can be important. WSU Public Data is explicitly or implicitly approved for distribution to the public without restriction. Examples of WSU Public Data include, but are not limited to, the following:

   a) Information provided on the University's public website;

   b) Information approved for release by the Registrar's Office that has been deemed "Directory Information," as defined by the University in accordance with the Family Educational Rights and Privacy Act (FERPA);

c) Course descriptions;

d) Semester course schedules; or

e) Press releases and openly accessible publications.

2. **WSU Campus Data.** WSU Campus Data is information that has a low level of sensitivity but is intended only for students, on-campus industry partners, University personnel, and Controlled Affiliated Organizations. Examples of WSU Campus Data include, but are not limited to, the following:

a) Campus Announcements not for public use such as upgrades, security changes and downtime notifications; or

b) Instructional information related to the education process that is not public in nature, such as class-wide announcements for systems access.

3. **WSU Private Data.** WSU Private Data is information that has low to moderate sensitivity and that is intended for internal University business use only, with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need to use or access the information. Unauthorized disclosure could adversely impact the University, Controlled Affiliate Organizations, third parties, or individuals. Examples of WSU Private Data include, but are not limited to, the following:

a) Financial accounting data that does not also contain WSU Restricted Data;

b) Departmental intranet;

c) Information technology transaction logs;

d) MyWSU ID;

e) Information security logs;

f) Directory information for students, faculty, and staff who have requested non-disclosure, such as students opting out under FERPA; or

g) Non-directory information or student records that are protected under FERPA, which includes information that is directly related to a student and maintained by an educational institution or by a party acting for the agency or institution.

4. **WSU Restricted Data.** WSU Restricted Data is highly sensitive information maintained, collected, or recorded by WSU that is intended for limited, specific use by a workgroup, department, group of individuals, or third party (typically pursuant to a contract or agreement) with a legitimate need to use or access the data. Explicit authorization by the designated Data Owner is required for access to WSU Restricted Data because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business or research functions of the University, affiliates, or external parties and violate the personal privacy of individuals, federal or state laws and regulations, or contractual obligations of the University. Examples of WSU Restricted Data include, but are not limited to, the following:

    a) Sensitive Personally Identifiable Information (SPII): There are two classes of SPII. The first class includes SPII that is sensitive regardless of whether any other identifier is paired with it ("Stand-Alone"). The second class of SPII becomes sensitive when it is combined with other types of Personally Identifiable Information (PII). The following are examples of each type of SPII:

        i. Stand-Alone SPII:

            (a) Social Security, driver's license, state ID, alien registration, or passport numbers;
            (b) Financial Account Number or credit/debit card numbers;
            (c) Identifiable Genetic Information and Biometric Identifiers;
            (d) Data of a known child (less than 13 years of age); or
            (e) Federal Tax Information

        ii. SPII when paired with other PII (such as a name or identification number):

(a) Medical Records (personal health information not covered under HIPAA; identifiable FERPA treatment records);
(b) Citizenship or immigration status;
(c) Racial or ethnic origin;
(d) Religious or philosophical beliefs;
(e) Sexual orientation;
(f) Criminal records;
(g) Employment records;
(h) Date of birth;
(i) Precise geolocation or Internet Protocol addresses (IP addresses);
(j) Last four digits of Social Security Number;
(k) Mother's maiden name;
(l) Union Membership;
(m) Text Messages (unless the business holding them is the intended recipient of the text message); or
(n) Videos, audio, or pictures of a person taken when the person would have an expectation of privacy (i.e., treatment videos taken in a clinic, etc.).

b) Protected Health Information (PHI) (including Designated Record Sets) held by Covered Entities or researchers at WSU;

c) Controlled Unclassified Information (CUI);

d) Information or data classified as "For Official Use Only" (FOUO);

e) Information or data subject to federal export control regulations; or

f) Facilities and Technology Control Plans.

D. **Classification and Safeguards Specified by a Third Party**

1. **Third-Party-Owned Proprietary Data.** Any classification and security standards for Proprietary Data that is owned by a third party, such as an individual, corporation, or government agency, will be specified by the third-party owner. The following are examples of proprietary data:

a) Data classified as proprietary, confidential, or a trade secret in a non-disclosure agreement, contract, or proprietary information agreement.

b) Data labeled as proprietary, confidential, or a trade secret.

c) Data regarded as a "trade secret" as defined by the Kansas Uniform Trade Secrets Act, KSA 60-3320, *et seq*

2. **Classified National Security Information (CNSI).** Any classification and security standards for data classified by the federal government as CNSI will be specified by the federal government in accordance with the National Industrial Security Program Operating Manual (32 CFR Part 117).

E. **Compliance with Laws and Policies.** University Data may be governed by state and/or federal laws, regulations, executive orders, guidance, or other policies. Data Owners must ensure compliance not only with University policies and all security safeguards required by University Information Security, but also with any state and/or federal requirements that govern the University Data for which they are responsible. The following are some examples of University Data that are subject to additional requirements:

1. SPII may be governed by state privacy laws, the Common Rule (protection of human subjects), the Gramm-Leach Bliley Act (financial information), and FERPA (student information). Employees should refer to Policy 3.12 / Security and Confidentiality of Student Records and Files for further information on the confidentiality of educational records.

2. PHI is governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Employees should also refer to Policy 20.17 Protected Health Information for further information on the safeguarding of PHI.

3. CUI is regulated by the National Archives and Record Administration in accordance with federal Executive Order 13556 and 32 CFR Part 2002. CUI shall be labeled according to CUI Markings standards set forth by the National Archives and Record Administration in addition to any other data labels required by this policy.

4. Scientific or technical information may be subject to federal export control regulations, International Traffic in Arms Regulations, 22 CFR Parts 120-130 and Export Administration Regulations, 15 CFR Parts 730-774). Employees should refer to Policy 9.21 / Compliance with Federal Export Regulations for further information on export control information.

F. **Data Protection**

1. **Data Security Safeguards.** University Data must be protected in accordance with this policy and all security safeguards as required by the University Information Security department, and in accordance with all governing state and federal requirements. All University Data shall follow the concepts of Least Privilege and Need to Know.

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.

IV. DEFINITIONS

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

1. **Biometric Identifiers:** Personal data resulting 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 natural person and that are used for identification purposes. Examples include facial recognition, iris recognition, fingerprint, voice recognition, hand geometry, behavior characteristics, retina scan, typing rhythm, and gait.

2. **Controlled Affiliated Organizations:** Wichita State University Intercollegiate Athletic Association, Inc., Wichita State University Union Corporation, Wichita State University Innovation Alliance, Inc., and WSIA Investments Corporation. Controlled Affiliated Organizations do not include Non-Controlled Affiliated Organizations.

3. **Controlled Unclassified Information (CUI):** Information that is recognized by the National Archives and Records Administration as requiring safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not

classified under Executive Order 13526 or the Atomic Energy Act, as amended.

4. **Covered Entity:** A health plan, health care clearinghouse or health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA.

5. **Data Custodian:** An Employee(s), department, division, or unit of the University who has been entrusted by a Data Owner with responsibility for the maintenance and protection of a collection or set of University Data at an administrative and/or operational level.

6. **Data Owner:** An Employee(s), department, division, or unit of the University who has created or is responsible for a collection or set of University Data, including the proper handling and protection of that University Data.

7. **Designated Record Set:** A group of records maintained by or for a Covered Entity that is: (a) the medical records and billing records about individuals maintained by or for a covered health care provider; (b) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (c) used, in whole or in part, by or for the Covered Entity to make decisions about individuals. For purposes of this definition, a record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a Covered Entity.

8. **Employee:** An individual who provides services to the University on a regular basis in exchange for compensation and receives a W-2 for such services. This includes temporary and part-time Employees.

9. **Financial Account Number:** A unique string of numbers, letters, and other characters that identify a specific financial account, such as routing numbers, checking or savings account numbers, mutual fund or annuity account numbers.

10. **Genetic Information:** Information about an individual's genetic tests, the genetic tests of an individual's family members, or the manifestation of a disease or disorder of an individual's family members. Genetic Information also includes an individual's request for, or receipt of, genetic services, or the participation in clinical research that includes genetic services by the individual or a family member of the individual, and the genetic information of a fetus carried by an individual or by a pregnant woman who is a family member of the individual and the genetic information of any embryo legally held by the individual or family member using an assisted reproductive

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.

V. 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.

VI. 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.

VII. APPLICABLE LAWS AND ADDITIONAL RESOURCES

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

B. Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191 (1996); 45 CFR Part 160 and Subparts A and E of Part 164)

C. Gramm-Leach-Bliley Act (P.L. 106-102, 113 Stat. 1338 (1999))

D. Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-2523)

E. International Traffic in Arms Regulations (22 CFR Parts 120-130)

F. Export Administration Regulations (15 CFR Parts 730-774)

G. Protection of Human Subjects (Common Rule) (45 CFR Part 46)

A. Executive Order 12958: Classified National Security Information, As Amended, March 2003

B. Executive Order 13556: Controlled Unclassified Information; 32 CFR Part 2002.

C. NIST Special Publication 800-171, Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

D. NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

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