



WSU POLICY APPROVAL COVER PAGE

DATE POLICY REQUEST TO PET:	August 2, 2022		
IS THIS A NEW POLICY OR CHANGE TO AN EXISTING POLICY?	NEW	<input checked="" type="checkbox"/>	EXISTING
CURRENT POLICY TITLE:	19.18 Third Party Data Transfers		
REVISED POLICY TITLE:	N/A		
LAST REVISED DATE OF POLICY:	N/A		
INITIATING AUTHORITY:	Information Security / Chief Data Officer		
SUMMARY OF POLICY OR POLICY CHANGE:			
This policy sets forth the requirements for the transfer of university restricted information.			
REASON OR NEED FOR POLICY / SUMMARY OF CHANGES MADE TO EXISTING POLICY:			
State of Kansas Information Technology Security Standard (ITEC) 7230A requires all state of Kansas agencies, including WSU, to employ mechanisms to ensure the confidentiality, availability and integrity of Restricted-Use Information. Pursuant to ITEC 7230A, "Restricted-Use Information" includes personal financial information (PFI), personally identifiable information (PII), and protected health information (PHI). Creation of a specific policy for transfer of Restricted-Use Information was also noted as an area of improvement for WSU during the university's most recent LPA.			
APPLICABLE LAWS OR REGULATORY OR POLICY AUTHORITY:			
State of Kansas Information Technology Security Standard (ITEC) 7230A			
OTHER RELEVANT WSU POLICIES:			
THE FOLLOWING UNIVERSITY STAKEHOLDERS WERE INCLUDED IN THE REVIEW AND APPROVAL OF THIS POLICY DRAFT / REVISION:			
	Office of the General Counsel – Misha Jacob-Warren		
	Information Security – Mark Rodee		
	Information Technology – Ken Harmon		
	Chief Data Officer – David Wright		
	IDP IT – Chris Synder		
OTHER NOTES FOR CONSIDERATION:			
N/A			
OWNER OF POLICY REQUEST FOR QUESTIONS:	Information Security / Chief Data Officer		

19.18 / THIRD PARTY DATA TRANSFERS

I. INITIATING AUTHORITY

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

II. PURPOSE

- A. The purpose of this policy is to decrease the risk around transmission and transfer of Restricted Information between the University and any Third Party.

III. POLICY

- A. Transfer of Restricted Information.
 - 1. All Data Transfers of Restricted Information shall be in accordance with Data Transfer Processes and Procedures.
 - 2. All Data Transfers of WSU Restricted Information from the University to a Third Party must be reviewed and approved by the DMC prior to transmission.
 - 3. All Data Transfers of IDP Restricted Information from the University to a Third Party must be reviewed and approved by IDP IT prior to transmission.
 - 4. All Data Transfers of Restricted Information that involve both WSU Restricted Information and IDP Restricted Information must be reviewed and approved by both the DMC and IDP IT prior to transmission.
 - 5. The DMC and/or IDP IT shall be notified thirty (30) days prior to renewal of any Data Use Agreements.
- B. Data Use Agreements.
 - 1. All Data Transfers of Restricted Information must be accompanied by a Data Use Agreement.
 - 2. All Data Use Agreements must be reviewed and approved by the Office of General Counsel.
- C. Termination of Transfer of Restricted Information
 - 1. Users must notify either the DMC (for WSU Restricted Information), IDP IT (for IDP Restricted Information), or both (for both WSU Restricted

Information and IDP Restricted Information) prior to termination of a Data Transfer to obtain transfer termination instructions.

2. The DMC and/or IDP IT may request termination of the transfer of Restricted Information and/or a Data Use Agreement.

I. DEFINITIONS

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

1. **Cloud Service:** Networked computing facility(ies) providing remote data storage and processing services via the internet. This can include but is not limited to Infrastructure as a Service (IaaS) or Software as a Service (SaaS) delivery methods and includes all cloud services, regardless of capacity.
2. **Controlled Affiliated Organizations:** Wichita State University Intercollegiate Athletic Association, Inc., Wichita State University Union Corporation, Wichita State University Innovation Alliance, Inc., WSIA Investments Corporation.
3. **Data Management Committee (“DMC”):** The University committee charged with managing and maintaining compliance with the Higher Learning Commission requirements related to institutional data for accreditation which includes but is not limited to providing oversight to University data systems to ensure data integrity, best practices in data management, reporting standards, information consistency, and security access.
4. **Data Transfer:** Automated or manual transfer of Restricted Information from the University to a Third Party. A Data Transfer may be a one-time transfer or an ongoing transfer. Data Transfers do not include: (a) University Restricted Information transferred under a sponsored research agreement, or (b) Restricted Information transferred under a legal request managed by the Office of General Counsel.
5. **Data Transfer Process and Procedures:** Those processes and procedures established by the DMC and/or IDP IT governing Data Transfers to Third Parties, which are published on the Information Security webpage, https://www.wichita.edu/services/information_security/.
6. **Data Use Agreement:** A contractual document used for the transfer of Restricted Information.
7. **IDP Restricted Information:** Includes all Restricted Information that is stored only within the NIAR Enclave.

8. **IDP IT:** The department / unit-specific technology office responsible for Industry and Defense Programs.
9. **NIAR Enclave:** The set of system resources that operate exclusively in the IDP security domain and that share the protection of a single, common, continuous perimeter.
10. **Third Party:** Any individual, organization, or entity that is not the University or a Controlled Affiliated Organization including, but not limited to a Cloud Provider.
11. **University:** Wichita State University and Controlled Affiliated Organizations.
12. **Restricted Information:** Includes all data, records, documents or files that contain information that is: (a) required to be maintained confidentially under any applicable law, regulation or University policy; (b) subject to a contractual obligation to maintain confidentiality; (c) subject to any applicable legal privilege or protection, such as the attorney-client privilege; (d) deemed by the University to be a trade secret, confidential or proprietary; and/or (e) classified by the University as WSU PRIVATE or above. Restricted Information encompasses both WSU Restricted Information and IDP Restricted Information.
13. **User:** Any individual, including but not limited to faculty, staff, students, contractors, and visitors who has access to and uses University information resources, systems or data.
14. **WSU Restricted Information:** Includes all Restricted Information that is not stored within the NIAR Enclave.

II. APPLICABLE LAWS AND ADDITIONAL RESOURCES

- A. Kansas Information Technology Security Standard (ITEC) 7230A