WSU POLICY APPROVAL COVER PAGE

DATE POLICY REQUEST TO PET:	[INSERT DATE]				
IS THIS A NEW POLICY OR CHANGE TO AN EXISTING POLICY?	**NEW**		**EXISTING**	**X**	
CURRENT POLICY TITLE:	19.18 Third Party Data Transfers				
REVISED POLICY TITLE:	N/A				
LAST REVISED DATE OF POLICY:	October 11, 2022 (approved but not published)				
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. This policy was initially approved by PET on October 11, 2022; however, upon further review it was determined that additional matters needed to be addressed prior to publishing, including specifying the type of data transfers that require the prior approval of the Data Management Committee and IDP IT, and clarification that some data transfers will not require an accompanying agreement that restricts the use of the data, such as protected student or medical information disclosed pursuant to a signed authorization and release.

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:

Kansas Information Technology Security Standard (ITEC) 7230A

OTHER RELEVANT WSU POLICIES:

WSU Policy 3.12 / Security and Confidentiality of Student Records and Files
WSU Policy 20.17 / Protected Health Information
WSU Policy 20.18 / Privacy of Financial Information

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

	Office of the General Counsel – Misha Jacob-Warren; Stacia Boden
	Information Security – Mark Rodee
	Academic Affairs – David Wright
	Faculty Senate – Jolynn Dowling (shared) [PENDING]
	Staff Senate – Jason Bosch (shared) [PENDING]

OTHER NOTES FOR CONSIDERATION: This is a compliance policy.		
OWNER OF POLICY REQUEST FOR QUESTIONS:		Information Security / Chief Data Officer

Policies and Procedures

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. Data Transfer of Restricted Information

1. All Data Transfers of IDP Restricted Information or WSU Restricted Information shall be in accordance with this policy and applicable 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 Data Management Committee ("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, as applicable, shall be notified thirty (30) days prior to renewal of any Restricted Use Agreements.

B. Restricted Use Agreements

1. All Data Transfers of Restricted Information must be accompanied by a Restricted Use Agreement, unless otherwise set forth in this policy.

2. All Restricted Use Agreements must be reviewed and approved by the Office of General Counsel.

3. Restricted Information may be transmitted without a Restricted Use Agreement if the Restricted Information includes:

   a) student educational records protected by the Family Education Rights and Privacy Act (FERPA) and is being produced to the student, or a third party authorized by the student, pursuant to a valid FERPA authorization and release, or as otherwise permitted under FERPA;

   b) patient records protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and is being produced to the patient, or a third party authorized by the patient, pursuant to a valid HIPAA authorization and release, or as otherwise permitted under HIPAA;

   c) confidential personnel records and is being produced to the employee, or an third party authorized by the employee, pursuant to a valid authorization and release; or

   d) records that are requested or compelled by court order, subpoena, or otherwise mandated to be produced under the law.

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 Restricted Use Agreement.

IV. DEFINITIONS

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

1. **Bulk Data:** An electronic collection of data composed of information from multiple records, whose primary relationship to each other is their shared origin from a single or multiple databases.

2. **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.

3. **Controlled Affiliated Organizations:** Wichita State University Intercollegiate Athletic Association, Inc., Wichita State University Union Corporation, Wichita State University Innovation Alliance, Inc., WSIA Investments Corporation.

4. **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.

5. **Data Transfer:** Automated or manual transfer of Restricted Information from the University to a Third Party that involves the following agreements and/or situations: (1) agreement for the purchase or use of Cloud Services for data storage, transfer, or processing; (2) agreement with a third party to manage, store, or transmit Restricted Information on behalf of the University; (3) agreements that require the University to set up a connection with a third party to University systems to receive or store data; or (4) any agreement or request for a transfer of data via the Internet that is outside of the normal business process, such as a first-time transfer of Bulk Data. 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 or expressly approved by the Office of General Counsel.

6. **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.

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. **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.

11. **Restricted Use Agreement:** A Restricted Use Agreement shall include any written agreement with the University that contains restrictions on the use and disclosure of the Restricted Information being transmitted, including, but not limited to, non-disclosure provisions, nondisclosure and confidentiality agreements, business associate agreements, and data use agreements.

12. **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.

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

14. **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.

15. **WSU Restricted Information:** Includes all Restricted Information that is not stored within the NIAR Enclave.

V. APPLICABLE LAWS AND ADDITIONAL RESOURCES

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

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

C. WSU Policy 20.17 / Protected Health Information

D. WSU Policy 20.18 / Privacy of Financial Information

VI. REVISION DATES

A. [INSERT PET APPROVED DATE]

Wichita State University Policies and Procedures

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. **Data Transfer of Restricted Information~~.~~**

1. All Data Transfers of IDP Restricted Information or WSU Restricted Information shall be in accordance with this policy and applicable 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 Data Management Committee ("DMC") prior to transmission.

3. All Data Transfers of ~~Industry Defense Programs ("~~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, as applicable, shall be notified thirty (30) days prior to renewal of any ~~Data~~Restricted Use Agreements.

B. **~~Data~~Restricted Use Agreements~~.~~**

1. All Data Transfers of Restricted Information must be accompanied by a ~~Data~~Restricted Use Agreement, unless otherwise set forth in this policy.

2. All ~~Data~~Restricted Use Agreements must be reviewed and approved by the Office of General Counsel.

3. Restricted Information may be transmitted without a Restricted Use Agreement if the Restricted Information includes:

a) student educational records protected by the Family Education Rights and Privacy Act (FERPA) and is being produced to the student, or a third party authorized by the student, pursuant to a valid FERPA authorization and release, or as otherwise permitted under FERPA;

b) patient records protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and is being produced to the patient, or a third party authorized by the patient, pursuant to a valid HIPAA authorization and release, or as otherwise permitted under HIPAA;

c) confidential personnel records and is being produced to the employee, or an third party authorized by the employee, pursuant to a valid authorization and release; or

d) records that are requested or compelled by court order, subpoena, or otherwise mandated to be produced under the law.

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~~Restricted Use Agreement.

~~I.~~IV. DEFINITIONS

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

1. **Bulk Data:** An electronic collection of data composed of information from multiple records, whose primary relationship to each other is their shared origin from a single or multiple databases.

~~1.~~2. **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.~~3. **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.~~4. **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.~~5. **Data Transfer:** Automated or manual transfer of Restricted Information from the University to a Third Party~~.~~ that involves the following agreements and/or situations: (1) agreement for the purchase or use of Cloud Services for data storage, transfer, or processing; (2) agreement with a third party to manage, store, or transmit Restricted Information on behalf of the University; (3) agreements that require the University to set up a connection with a third party to University systems to receive or store data; or (4) any agreement or request for a transfer of data via the Internet that is outside of the normal business process, such as a first-time transfer of Bulk Data. 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 or expressly approved by the Office of General Counsel.

~~5.~~6. **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/.~~Information Security webpage.

~~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.~~1. ~~**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.~~1. ~~**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;

10. (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.~~

11. **Restricted Use Agreement:** A Restricted Use Agreement shall include any written agreement with the University that contains restrictions on the use and disclosure of the Restricted Information being transmitted, including, but not limited to, non-disclosure provisions, nondisclosure and confidentiality agreements, business associate agreements, and data use agreements.

12. **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.

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

~~13.~~14. **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.~~15. **WSU Restricted Information:** Includes all Restricted Information that is not stored within the NIAR Enclave.

~~II.~~V. APPLICABLE LAWS AND ADDITIONAL RESOURCES

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

~~B. WSU Policy: 3.12 / Security and Confidentiality of Student Records and Files~~

~~C. WSU Policy: 20.17 / Protected Health Information~~

A. ~~WSU Policy: 20.18 / Privacy of Financial Information~~Kansas Information Technology Security Standard (ITEC) 7230A

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

C. WSU Policy 20.17 / Protected Health Information

D. WSU Policy 20.18 / Privacy of Financial Information

VI. REVISION DATES

A. [INSERT PET APPROVED DATE]

~~D.~~