Restricted Use Data Policy
For Third-Party Service Providers

I. Policy Statement

Third-Party Service Providers ("TPSPs") play an important role in the support of WPI processes. In some instances, TPSPs have access (e.g., collect, store, and maintain) to WPI Restricted Use Data. This policy aims to mitigate the risk of permitting Restricted Use TPSPs to have access to Restricted Use Data by setting forth obligations of WPI personnel who are responsible for hiring and managing the work of Restricted Use TPSPs. This policy seeks to improve compliance with data breach regulations, and reduce the risk of security incidents, financial liability and loss of community trust.

II. Scope

This policy applies to all WPI Project Supervisors.

III. Definitions

"Restricted Use Data" has the same meaning as it is defined in WPI's Data Classification and Usage Policy.

"Restricted Use Third-Party Service Providers (TPSPs)" means an entity (e.g., a person or a company) under contract with WPI to provide services to WPI and that involve access to Restricted Use Data.

"Third-Party Service" means a service provided by a Restricted Use Third-Party Service Provider.

"WPI Project Supervisor" means the WPI employee(s) who is responsible for managing the relationship with the Restricted Use TPSP and the Third Party Services it provides.

IV. Policy

A. Contracts

Any WPI Project Supervisor(s) who intends to engage a Restricted Use TPSP must follow applicable WPI policies for hiring such a vendor. This may include performing the appropriate due diligence prior to selection, including obtaining approval through Administrative Services Working Group (ASWG). Additionally, the contract must be reviewed carefully and, when applicable, in consultation with WPI's Office of the General Counsel, prior to its execution.

B. WPI Responsibilities

The WPI Project Supervisor is responsible for ensuring that the Restricted Use TPSP('s):

1. Provides a specific point of contact for implementation and service offering. A designated WPI point of contact will work with the Restricted Use TPSP to ensure the Third-Party Services are in compliance with all state and federal laws, as well as this policy.

2. Completes and submits to WPI's Chief Information Security Officer (CISO) a Higher Education Community Vendor Assessment Toolkit (HECVAT) to assess security practices which will be reviewed by the CISO.

3. Is vetted and approved through the Administrative Services Working Group (ASWG) security approval process prior to performing any Third Party Services.

4. Meets or exceeds WPI's requirements for data privacy, information security, and the return, destruction, or disposal of information in their possession per the terms of the contract.

5. Staff members assigned to provide the Third Party Services to WPI and who have access to Restricted Use Data (a) are cleared to handle that information, (b) have access only when necessary and enabled only to the level and degree required to perform the Third Party Services, (c) have uniquely identifiable access to Restricted Use Data and comply with all WPI password and access management requirements, (d) are appropriately monitored during use as necessitated by the sensitivity and confidentiality of the information, (e) use only the prescribed tools and procedures to access systems remotely, as applicable, (f) immediately report any and all security incidents directly to the WPI Project Supervisor and the CISO, (f) follow all applicable WPI change control processes and procedures, and (g) have their access to Restricted Use Data deactivated/disabled upon termination of the contract and/or after Third-Party Services have been completed.

6. Upon termination of the contract, the Third Party Service, and/or at the request of WPI (a) return or destroy all information (including Restricted Use Data) and provide written certification of that return or destruction within twenty (24) hours of the termination or request, and (b) surrender all identification badges, access cards, equipment, and supplies immediately and document any equipment and/or supplies to be retained by the Restricted Use TPSP.

Additionally, the CISO shall maintain a list of all Restricted Use TPSPs and the Third-Party Services performed by each.

V. Related Policies

Related Policy - Data Classification and Usage Policy

VI. Questions

If you have any questions regarding this policy, please contact WPI's Chief Information Security Officer at CISO@wpi.edu.

* * *

Policy Sponsor: Chief Information Security Officer
Responsible Department: Information Technology
Effective Date (i.e., date of Presidential Approval): April 19, 2021