

Baldwin Wallace University Information Technology Standard

Issued by:	Information Technology
Title:	Data Dissemination
Number:	ITS-BW-04-02
Publish date:	June 1, 2022

A. Data Request and Dissemination Process

To obtain or disseminate sensitive data, as defined by ITP-BW-04 Data Classification Policy, to which a person does not have direct access to requires a Data Governance Request form to be completed and approved before any action is taken.

Example: An HR professional has direct access to sensitive data about employees. The HR professional does not need to complete a Data Governance Request form each time he/she accesses the sensitive information as that is part of their normal job function. However, if the HR professional intends to disseminate that same sensitive information to those that do not have electronic access to that data, then a Data Governance Request form must be completed and approved.

Types of Data Governance Requests:

There are two types of Data Governance Requests.

One-Time Request:

A One-Time request is for a report of data that is ad-hoc in nature and may or may not be repeated in the future.

Standard Request:

Standard requests are for specific reports of data that will be repeated on a predictable and repeating pattern using the same format and data elements. It will also be delivered to the same application, cloud service, or job position (NOTE: the person may change, but not the job position) each time. Standard requests need only to be approved once and do not require renewal unless there is a change to the report, data elements used, application, cloud service, or job position delivered to. Any change to the initial request, no matter how small, requires the Standard Request to be reapproved.

Example: A specific report on students that contain sensitive information is to be created each semester and delivered to a specific job position in the university. Once approved, reapproval is not required, and the report may be generated and disseminated semester after semester. If an additional data element is added to the report, then reapproval is required before the report can be issued again. Similarly, if the job position the report is delivered to changes or the pattern of when the report is generated changes, then reapproval is required.

B. Value-Based Risk Approval Requirements

The level of risk associated with data is defined by ITP-BW-04 Data Classification Policy and ITS-BW-04-01 Data Classification Standard. Based on those levels of defined risk, the approval requirements for a Data Governance Request form are defined as shown in the chart below.

Classification Category		Approval Levels Required
3	Restricted	Data Governance Request Form Requires approval by the Data Owner (or their designate) AND one of the following: CIO, CISO, or DPO
2	Confidential	Data Governance Request Form Requires approval by the Data Owner (or their designate) AND one other member of the Data Governance Team
1	Internal	Data Governance Request Form Requires approval by the Data Owner (or their designate) only
0	Public	Data Governance Request Form approved by any Data Governance Team member

C. Approval Documentation

The approval process must document when and who approved each request such that clear and indisputable attribution of the approver(s) is guaranteed.