UNIVERSITY OF MINNESOTA
Driven to Discover℠

Sharing Enterprise Data Checklist

The following checklist should be used each time a sharing data request is received to determine if University data can be shared internally and externally, and how to help ensure the data is shared in compliance with data privacy laws and the following University policies and procedures:

External Audiences: Sharing Data with Audiences External to the University Procedure
Public Access to University Information
Internal Audiences: Sharing Data with Audiences Internal to the University Procedure

When in doubt, direct any external requests for data through the Data Request Center, or contact the Data Custodians who are available to help answer your questions.

- ❏ Determine if you have a University business need to access this data
  - If no/unsure, consult with a Data Custodian to determine access options
- ❏ Determine if the recipients are internal or external to the University
  - If an internal audience acting as a School Official with a business need to receive data: follow the Sharing Data with Audiences Internal to the University Procedure or refer internal requests to the Data Custodian
  - If an external audience: follow the Sharing Data with Audiences External to the University Procedure or refer external requests to the Data Request Center or to the Data Custodian
- ❏ Determine the Data Security Classification of each data element by consulting with the Data Owner or Data Custodian or through the Term Glossary (requires a VPN connection)
  - Examples: Data Security Classifications by Type
- ❏ Determine which Data Privacy policies and laws apply to the data
  - If the data includes Student elements, FERPA training is required prior to sharing. Private-restricted student data cannot be shared with third parties; directory information is suppressible and most student data is private-restricted
- ❏ Determine if it is appropriate to share dynamic real-time data or official static (snapshot) reports
  - Official University (snapshot) reports should be used whenever appropriate
  - Dynamic reports should be used to generate custom results (MyU Reporting Center, Institutional Data and Research)
- ❏ Determine the minimum data necessary to meet the business need or data request
  - If an internal audience, verify the requestor has the appropriate data access roles and/or completed the required data trainings to receive the data
  - If an external audience, apply the Data Suppression “Rule of 10”, based on summary level and data security classification
- ❏ Additional considerations
  - Data should be shared and stored in accordance with University storage and retention guidelines
  - Include a ‘data as of’ date
  - Use data in alignment with University data definitions and business rules

Resources

- Enterprise Data Management & Reporting (edmr@umn.edu)
- Data Access and Privacy Office (ogcweb@umn.edu)
- University Policy Library
- Sharing Enterprise Data Training Course
- University Information Security (security@umn.edu)