Data Management Group

The Data Management Group (DMG) oversees the access and use of data at VT

Table of Contents

Data Management Group Overview

The Data Management Group (DMG) is composed of data stewards and IT staff who support data management (formerly Data Custodians) and/or their designees. Data Stewards are appointed by, and accountable to, the Data Trustees for the designated data domain.

Membership
The standing DMG data steward membership consists of the data stewards for the domains that together represent the coverage of all fundamental person categories plus finance data:

- Students
- Alumni
- Employees
- Affiliates

The standing DMG Data Stewards can appoint rotating/ad hoc member(s) of additional Data Stewards at their discretion. The IT staff membership in the group are also at the discretion of the standing DMG Data Stewards but should consist of those IT leaders or staff than can answer questions about the relevant data, surrounding processes, and usage or implications as well as those that will be directly involved in executing the decisions of the DMG.

The DMG works together to standardize data management practices across domains and ensures that data is managed as a material asset, data provides value, meets compliance requirements, and risks are managed appropriately.

DMG Multi Domain Data Access Approval Process

Decisions about new uses of multidomain data (data that crosses more than one domain) are made by the DMG. The data management group is composed of the data stewards (the delegates of the data trustees) from each core domain and representatives from IT groups to assist with questions. Data Stewards of other domains or subdomains may be included as needed depending on the request. Decisions are made by the data stewards or data trustees. The group typically meets on a monthly basis to discuss data issues. In the event of a more urgent need for discussion, the group may choose to discuss via email or call an out-of-cycle meeting.

As the DMG group only meets monthly, requestors should plan ahead in their projects and come well prepared to avoid a need for a second meeting. If you have any questions about preparing for a DMG meeting, contact {email}.

If a project involves a new use of multidomain data or a system or process change that will impact multiple data domains, then requestors should complete the following process.

Multi Domain access request process steps:

1. **Request**

a. Complete the multi domain data access request form - {FORM}.
    i. Requests that only involve the release of data for a single data domain only require the approval of the relevant data steward and do not need to be submitted to the DMG.
b. Email the form to Secure Identity Services - {email}.

2. Validation

a. Secure Identity Services will review the request and may ask for additional details or clarification from the requestor.
b. Secure Identity Services will validate:
    i. That any data access prerequisites by the data stewards have been met.
    ii. Whether any relevant contracts have FERPA clauses.

3. Approval

a. Secure Identity Services will add the request to the next DMG agenda or schedule an out-of-cycle approval review as needed.
b. Secure Identity Services will contact the requestor with meeting details.
c. The requestor and other relevant individuals will attend the DMG meeting for discussion.
d. Which Data Stewards in the DMG need to approve is determined by the scope of the data request consistent with the Standard for Administrative Data Management.
e. The DMG will provide a decision or may request additional information/tasks.

4. Notification

a. Secure Identity Services will send notification of the approval results to the requestor.

5. **Implementation**

    a. Secure Identity Services, Enterprise Services, or relevant IT groups will provide access to the relevant data by the means approved by the data stewards.

6. **Archive**

    a. Secure Identity Services will archive the request and results.
    b. Archive method and repository TBD.

DMG Responsibilities

The DMG will be responsible for the following across data domains OR where data consists of multiple data domains. The role of the DMG does not subsume or override roles or authority established in the Standard for Administrative Data Management, rather it provides a structure for the Data Stewards to work collaboratively, and exercise joint authority especially over matters involving multiple data domains.

- Multi Domain Data Risk Management
    - Managing risk to multi domain data including escalating any identified significant risk to data trustees and advising data trustees on risk acceptance decisions
- Multi Domain Data Access
    - Defining prerequisites or other requirements related to access to multi domain data

    - Defining access, quality, and usage guidelines for multi domain data
    - Reviewing and approving or denying requests for access to multi domain data
    - Commissioning data access reviews, data security audits, or other work relates to data access
    - Constructing business access that dictates security procedures and rules for third-party usage of system data
- Coordinating Standardization
    - Give guidance on standard approaches and ensure that best practices are shared across the steward group
    - Data quality processes and controls
    - Processes to ensure confidentiality, integrity, availability, and usefulness of data
- Education
    - Sharing best practices in regard to data governance with respective stakeholders

DMG Evaluation Considerations

- Authority and purpose for data collection including:
    - determine the legal bases that authorize a particular personally identifiable information (PII) collection or activity that impacts privacy
    - provide adequate notification of the purpose(s) for which PII is collected
- Accountability, audit, and risk management of data to ensure effective controls for governance, monitoring, and mitigation to demonstrate that

units are complying with applicable privacy protection requirements and minimizing overall privacy risk.

- Data quality and integrity processes to ensure that highly critical data is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices and in support of the university's strategic objectives.
- Data minimization and retention processes so that the university collects, uses, and retains only personally identifiable information (PII) that is relevant and necessary for the purpose for which it was originally collected.
- Individual participation and redress processes so that individuals are active participants in the decision-making process regarding the collection and use of their personally identifiable information thus enhancing public confidence.
- Transparency by providing public notice of information practices and the privacy impact of programs and activities.
- Guidelines and processes to ensure that the use of personally identifiable information (PII) is limited either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law.

Appendix A - Membership of the DMG

Data Stewards

- **Student Data:** Rick Sparks - University Registrar
- **Alumni Data:** Rhonda Arsenault - AVP for Advancement and COO
- **HR/Employee Data:** Marie Bliss - AVP, HR Administration
- **Finance Data:** Melinda West - AVP for Finance & Controller
- **Affiliate and Identity Data:** Ryan McDaniel - Executive Director, SIS

IT Data Support

- **Identity and Access Management:** Kevin Rooney
- **ERP Access/Security:** Rhonda Randel
- **Enterprise Systems:** Allen Campbell

Appendix B - Data Steward Responsibilities

As described in:
Administrative Data Management and Access Policy - 7100

Data Stewards - University officials (typically at the level of Associate Vice President, Associate Vice Provost, University Registrar, University Bursar, or Director) who oversee the capture, maintenance and dissemination of data for a particular operation. Data Stewards are appointed by the respective Data Trustee. Data Steward responsibilities include risk classification of data based on any legal, ethical, or externally imposed constraint; documenting the process for approving and reviewing access; defining controls related to the confidentiality, integrity, and security of the data; and other activities assigned by a Data Trustee.

Standard for Administrative Data Management:

- 1.2 Data Stewards
    - Data Steward responsibilities are assigned by the data trustees
    - These responsibilities include:
        - Classifying data for access and sensitivity
        - Define and monitor data quality
        - Craft and communicate data definitions
    - Data stewards are:
        - The primary contacts for members of the university community with regard to data in their domains.
- 1.3 Other Roles
    - Data stewards often direct data experts, custodians, and data managers.
- 2. Data Domains
    - Data stewards are needed for purposes of:
        - requesting access
        - Handling requests for data corrections
        - Understanding data definitions, classifications, and sensitivity

Guidelines for Data Stewards:

- Work with the relevant Data Trustee and Information Technology Security Office to assure that data is classified by the Virginia Tech Risk Classifications low, moderate, or high risk. Identify procedures for maintaining data confidentiality as they relate to data under the Data

Steward's management. As needed, work with the IT Security Office to enforce the procedures.

- Assure that there are documented and published processes for granting access to data for appropriate university business units.
- Review and respond to requests for data based upon legitimate university business objectives that would benefit from the use of requested data. As needed, obtain a signed Memorandum of Understanding from the Director of a department requesting the ability to extract or use data from a system under the Data Steward's management.
- Work with Information Technology Security Office to validate that all systems, including externally hosted systems supporting business processes within the Data Steward's area, conform to Virginia Tech’s standards for security and data handling.
- As needed, participate in the management of shared data in ERP systems (such as Banner) supporting the Data Steward's business area.
- Establish and maintain an appropriate structure and review process for responsible management of data access.
- Communicate to stakeholders regarding the enterprise use, policies and decisions around the stewarded data.
- Communicate for stakeholders in a way that represents their perspectives within the domain of stewardship.

Appendix C - Terms and Concepts

Data Governance
Data governance is the orchestration of people, processes, and technology to manage the company's critical data assets by using roles, responsibilities, policies, and procedures to ensure the data is accurate, consistent, secure, and aligns with overall company objectives. - Hallmark/Gartner

Stewardship Model
A business-led model that directs and advises users across the enterprise to ensure that data-related work is performed according to policies and procedures as established through governance. - Hallmark/Gartner

Data Steward
An individual with formal accountability and responsibility to define, control and maintain data and business rules within their domain … responsible for guiding the effort to execute the policies and procedures as established by Data Governance. - Hallmark/Gartner

<u>Work Tasks:</u>

- Assess the current state of data fidelity, security, privacy and retention within their scope of responsibility.
- Interpret and enforce activities to ensure target goals for data fidelity improvement and adherence with all other types of data governance policies.
- Identify optimal approaches for resolving data quality or consistency issues to achieve targets.
- Work within and beyond their immediate area to implement change in support of the adoption of data governance policies.
- Monitor and track ongoing data fidelity (e.g., quality and consistency) levels and other metrics that assess the adherence of data and people to data governance policies.

- Report into the data governance council either via the lead data steward, or as a team (a data stewards group, for example, where the need for stewards spans data domains and business functions), or individually (per their direct responsibility).
- Actively correct data quality flaws that cannot be addressed fully by automated means.

Data Custodian

Data Stewards are commonly responsible for data content, context, and associated business rules. Data Custodians are responsible for the safe custody, transport, storage of the data and implementation of business rules. Maintains data requirements and definitions. Controls data access and usage. Monitors data quality. Simply put, Data Stewards are responsible for what is stored in a data field, while Data Custodians are responsible for the technical environment and database structure. Common job titles for data custodians are Database Administrator (DBA), Data Modeler, and ETL Developer.

Subject Matter Experts

Analyze data elements and definitions. Help identify authoritative sources of data. Establish processes to ensure data quality. Common job titles for SMEs are Business Analyst, Systems Analyst, etc.