Appendix B to the University of Virginia's College at Wise Information Sensitivity Policy

Roles and Responsibilities Related to College Administrative Data – These roles and responsibilities have been adopted by the University of Virginia's College at Wise from the University of Virginia with minor modifications to more accurately meet the needs of the College.

Roles at a Glance

Data Stewards - Senior University officials, or their department head level designate(s), with planning and policy-level responsibility and accountability for data, including creation and maintenance, within their appropriate data domains. They determine who may create, maintain, and use data in the domain area(s) for which they are responsible, and they are responsible for ensuring the quality of data entered.

Data security contacts – Carry out the data domain policies set by the data stewards, as well as the College's overall administrative data security policies; play major approval role in data access authorization processes.

Data users – View, copy or download data, but do not enter, modify or delete it.

Data processors – Enter, modify or delete data.

System Sponsors – Negotiate priorities and enhancements to the systems and lead change management processes in accord with the documented strategic goals for particular systems; responsible for ensuring that the system for which they serve as sponsor is operable and available to all authorized users on an established schedule.

Information Technology – Set strategic direction, develop overall policies, coordinate, and provide services supporting College-side data administration activities.

Roles include:

- **Chief Information Officer(s)** – Set policies, procedures, and guidelines for College-wide data administrative activities; establish security standards for administrative data, in order to promote and protect the College's interests in it.
- **Information Security Officer(s)** – Coordinate the College's overall IT security programs and ensure compliance with relevant Commonwealth security policies, standards and guidelines.
- **Data Administrator(s)** – Develop and apply standards for the management of institutional data and for ensuring that data are accessible to those who need it. They work closely with the data stewards on formulation of domain data policies, standards, and procedures.
- **Data Security administrator(s)** – Administer the data authorization process for enterprise-wide administrative data.

Detailed Descriptions

Data Stewards

Data stewards are senior College officials, or their department head level designate(s), who have planning and policy-level responsibility and accountability for data, including creation and maintenance, within their appropriate data domains.

Specific responsibilities include:

1. Assigning each item of administrative data to one of three categories: general administrative, legally restricted, or limited-access (see Appendix A).

2. Defining the criteria for archiving the data to satisfy mandated and business-driven retention requirements, with advice from system sponsors on the balance of cost effectiveness and reasonableness.
3. Determining the business needs for security for their data and monitoring and reviewing security implementation and authorized access, in consultation with the appropriate information security officer and system sponsor.
4. Establishing procedures for initial definition and change of data elements within their data domains.
5. Providing data descriptions for directories that will let data users know what shareable data are available, what the data mean, and how to access the data stored within the repositories for which they are responsible. Data definitions will be: based on actual usage, made according to College standards, modified only through approved procedures, and reviewed on a timely basis and kept current.
6. Developing policy to promote the accurate interpretation, responsible use and protection of administrative data in their domains.
7. Specifying data viewing, copying, or downloading procedures that are unique to a specific data repository or set of data elements. These procedures will ease "read-only" access, will preserve data quality and will minimize security risk.
8. Ensuring the rules and conditions that could affect the accurate presentation of data are well-known by data users and processors and supporting users/processors in the use and interpretation of administrative data, primarily through documentation, training, and problem resolution.
9. Ensuring data quality by:
    a. Determining the most reliable sources of data and regularly evaluating the quality of the data.
    b. Assigning and overseeing data entry, data capture and maintenance to ensure data quality.
    c. Identifying gaps and redundancies in the data and, to the extent possible, ensuring that only needed versions of each data element exist.
    d. Specifying data control and protection requirements to be observed by data processors and users.
    e. Informing the system sponsor of any new data needs, gaps in quality, and/or removal of data redundancies or obsolete data.
    f. Generally monitoring the data for accuracy, integrity, and dependability, and where appropriate, initiating action concerning these issues.

Data Security Contacts

Data security contacts carry out the data domain policies set by the data stewards, as well as the College's overall administrative data security policies. Data security contacts are responsible for making known the rules and procedures to safeguard the data from unauthorized access and abuse. They also play an active and critical role in data access authorization processes. Access in this context means either (a) the capacity for data processors to enter, modify or delete data or (b) the capacity for data users to view, copy or download data. The access-authorization responsibilities of data security contacts include:

1. Approving access requests for sponsored employees and non-UVa-Wise individuals within their departments and forwarding these to the next stop in the approval chain (varies with the application for which access is being requested).
2. Requesting adjustments to these authorizations when access needs of employees and non-UVa-Wise individuals within their departments change.
3. Regularly verifying the accuracy of existing authorizations for individuals in their departments and monitoring for inappropriate access activity.

Data security contacts who report to a data steward are typically also assigned responsibility for approving all or selected requests (varies with the system) from other departments to access data in that data steward's data domain. In some cases, such as the University of Virginia's Oracle applications, data stewards have granted blanket access for selected data on condition that the requestor satisfies certain prerequisites (e.g. signing a confidentiality agreement).

Data users are, in this context, any College/University employees who use UVa-Wise/UVA administrative data – persons who view, copy or download data, but who do not enter, modify, or delete it. Persons who view data and who copy or download it are responsible for the accurate presentation of that data. They also are responsible for helping to protect the data to minimize security risks and for helping to monitor data quality. For more details on data user responsibilities see Section 5.0 of the Information Sensitivity Policy.

Data processors are persons specifically authorized by data stewards to enter, modify, or delete data. They are responsible and accountable for completeness, accuracy, and timeliness of the data, and they are cognizant that other persons rely on their products for those qualities.

System sponsors ensure the usability, reliability, availability and integrity of information systems and their data by serving as liaisons between each system's stakeholders – all parties with interests in such systems. The system sponsors negotiate priorities and enhancements to the systems and lead change management processes in accord with the documented strategic goals for particular systems. They are responsible for ensuring that the system for which they serve as sponsor is operable and available to all authorized users on an established schedule. They also serve as liaisons between the stakeholders and the technical staff responsible for such systems and the infrastructure in which they operate. They notify technical staff and stakeholders of required changes. They provide resources and training to those with other data-related roles to assure that quality standards are met.

Information Technology set strategic direction, develop overall policies, coordinate, and provide services in support of the College-wide data administration activities. The responsibilities are encompassed in the follow roles:

- **Chief Information Officer** depending on the nature of the data involved, are individually responsible for setting overall policies, procedures, and guidelines for the College-wide data environment and infrastructure. They establish quality and security standards for administrative data, in order to promote and protect the College's interests in it. They also are ultimately responsible for defining and implementing policies to assure that College administrative data are recoverable from unforeseen lost or damage to the degree that can be accomplished at reasonable cost. The data stewards and system sponsors play active roles in assisting their relevant CIO in this responsibility. Also with the data stewards' and system sponsors' advice, the CIOs will develop workable plans for resuming operations in the event of a disaster, including recovery of data and restoration of needed computing infrastructure services.
- **Agency information security officers** are persons designated by the relevant CIOs (responsibility delegated from the Chancellor) to serve as the Commonwealth of Virginia-recognized information security officers. This role is responsible for coordinating the agencies' compliance with relevant Commonwealth security policies, standards and guidelines, notably SEC2000-01.1, Information Technology Security. In this role, each agency information security officer works in partnership with units and individuals across the College to establish strategic direction, review and recommend policy, provide security education and training, establish security safeguards, monitor for and address security incidents, assess risk, develop business continuation plans, and related activities.
- **Data administrators of IT and Computing Services** develop, communicate and monitor compliance with standards for the management of institutional data and for

ensuring that data are accessible to those who need it. They work closely with the data stewards on formulation of data policies, standards, and procedures. The data administrators work with the system sponsors and data stewards to establish long-term direction for effectively using information resources to support College goals and objectives. The data administrators develop the overall data architecture and create logical data models for data repositories. These models are ultimately used to create an institution-wide data model that cross-references data across applications and encourages data sharing. The data administrators develop standard methods for naming and defining data. They also facilitate conflict resolution in data definitions. They provide means that enable institutional data to be available to authorized users in a manner consistent with established data access rules and decisions. The data administrators develop, communicate and promote standards for data quality, as well as model-processes for assuring it. In conjunction with the agency information security officers, they develop and promote processes to minimize security risks.

- **Data security administrators of IT and Computing Services** work closely with data security contacts, and where appropriate Human Resources, to administer data authorization processes for enterprise-wide administrative data. They establish/delete user IDs and grant/remove access to users with proper authorization and manage password expiration and reset processes. They also distribute and monitor data security contact usage of administrative data security reports and investigate unauthorized access in collaboration with the UVa-Wise/UVA Audit Department, the Auditor of Public Accounts, and the UVa-Wise Police Department.