Title: Document Imaging Policy Policy: 6720

Purpose

The Virginia State University ("VSU") Document Imaging system shall be compliant with the Commonwealth's IT Security Standards, State Library of Virginia ("SLV") Records Retention and Disposition Schedules as well as best practices for planning, implementing, and management of electronically stored information.

Imaging systems procedures are required for all academic departments and administrative offices that create, use, and manage digital images in an imaging system. Imaging system processes are required in order to ensure validity and integrity of each record during image capture, storage, and reproduction.

Guiding Principles

The following principles guide the development and implementation of the VSU Document Imaging Policy:

A. eDiscovery Best Practices:

1. VSU must have the ability to adequately and responsibly respond to any legal actions that materialize. Furthermore, the need to have a management system in place for document images (regardless of scanned and/or faxed) furthers that objective.
2. VSU aims to protect the legal interests of the University and the Commonwealth of Virginia ("COV") by having a structured and effectively applied document imaging policy.

b. Legal Hold Procedure:

1. VSU fully intends to comply with any Legal Hold Order that may materialize. In order to assist in the proper segmenting and preservation of relevant document images, a document imaging policy is necessary to further the objective and aid to understanding.

c. Compliance with the State of Virginia Library Data Retention Requirements

1. Specifying the location, manner, and media in which electronic mail records will be maintained to meet operational and archival requirements.

Scope of Policy

This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators, and students) who access and/or utilize the information technology infrastructure owned or leased by VSU.

Document Imaging Statement

University document images are defined as any image scanned or printed, sent or received through the university's information technology infrastructure and via fax or copier. Such images include any departmental level images created between the user and the University document services.

Authority, Responsibility, and Duties

The IT Security program roles and responsibilities are assigned to individuals and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. Refer to Information

Security Policy 6110 for IT Security roles and responsibilities. Imaging system roles are defined as follows:

A. Data Owner

The Data Owner (user) is the University employee (contractor or state employee) responsible for the policy and practice decisions regarding his or her data and to ensure the privacy of information in their respective areas. More specifically:

1. Evaluate and classify sensitivity of the data in line with the University policy.
2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
3. Communicate data protection requirements to the System Owner.
4. Define requirements for access to the data.
5. Compliance with the state, federal, and privacy laws (i.e. HIPPA, FERPA, GLBA, etc.) on the data storage, retrieval, retention, and disposal.
6. Compliance with the State Library of Virginia policy and procedures on classification and retention of data.
7. Inform VSU Information Security Officer (ISO) and management of disclosure related to improper use and/or unauthorized access to sensitive data.
8. Communicate security and protection requirements in conjunction with information systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

B. System Owner

The System Owner of any/all document management and storage applications is responsible for policy duties relative to his or her system. Said duties include, but are not limited to:

1. Ensuring that the system users are adhering to the data classification and protection requirements that are established within University policies.
2. Communication of the Document Imaging Policy to the users of his or her system.
3. Compliance with the Document Imaging Policy in all aspects, including storage, retention, indexing and classification of documents.
4. Compliance with the state, federal, and privacy laws (i.e. HIPPA, FERPA, GLBA, etc.) on the data storage, retrieval, retention, and disposal.
5. Compliance with the State Library of Virginia policy and procedures on classification and retention of data.
6. Inform VSU Information Security Officer (ISO) and management of disclosure related to improper use and/or unauthorized access to sensitive data.
7. Communicate security and protection requirements in conjunction with information systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.
8. Ensure that only authorized users have access to the system and that said access is commiserate to the role and duties of the user within the University system.

Definitions

The IT security definitions and terms can be found in the COV ITRM IT Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/library.

The Library of Virginia definitions and terms can be found in the Public Records Management Manual Glossary. It is referenced on web page http://www.lva.virginia.gov/agencies!records/manuals/vprmm.pdf.

"Banner System" is the system used at VSU for the administrative and business activities of the University. Said administrative functions include but are not limited to the hosting of students' grades and transcripts, records and the like.

A "Multi-Function Copier" refers to a copy machine that is enabled to scan, print and fax documents and Images.

"Microfiche" refers to legacy documents that were originally scanned and stored on storage media known as films for microfiche.

Policy Statement

1. Each department using the imaging system must have procedures developed for scanning, quality assurance, labelled and classified, and verifying to ensure that scanned documents are an exact copy of the original. Said information within the image must be readable.

2. Each department must properly record the retention series and retention time for state and local documents and/or records in accordance with The State Library of Virginia Public Records Management Manual and Record Schedules as well as University policies.

3. Audit logs must be maintained for the imaging system, regardless of medium. Logs must be kept in a safe, access controlled location by the system owner for each system (i.e. Banner, Microfiche and the like).

4. Regardless of the system used for storage of document images, said records/images must be classified, labelled, and archived by the data owners based upon the classification designations below:

   Three general classes of information designations are:

   a. **Retained Records-** document images (scanned, faxed or otherwise) that contain content subject to State Library of Virginia records retention schedules, including but not limited to: content of a legal nature, considered a vital record, or has historical value.

   b. **Lasting Value-** document images (scanned, faxed or otherwise) that should be retained due to operational nature of the image content. Lasting value also describes document images (scanned, faxed or otherwise) under retention schedules for which the retention time period has lapsed.

   c. **Transitory Routine-** communication, scheduling, or any document images not deemed to have lasting value.

      Examples include meeting or event notices, internal requests for information, announcements, or unsolicited commercial faxes, etc. These documents do not have to be indexed and archived. These items shall be removed immediately once usefulness has expired.

5. This policy applies to the following systems: Multi-Function Copiers ("MFC"), Microfiche, Fax machines, flat scanners, and any other system capable of producing an image from paper documents. This policy applies to any document management system, regardless of whether it is Commercial Off-the-Shelf, Open Source, or VSU proprietary.

6. Data Owners (users) and System Owners should refrain from transmitting Personally Identifiable Information ("PII") or Protected Health Information ("PHI") images via any MFC, fax machine, or other electronic means.

7. It is the responsibility of the System Owner(s) to train the Data Owner(s) on the proper usage of any document storage management system within their control and dominion.

8. Document images shall not be stored on Data Owners or System Owners local computer drives or within email boxes.

9. It is the responsibility of the Data Owner and VSU Records Custodian to retain a backup of any document image that is deemed to be preserved under VSL retention policies, as well as, University policies.

A. Exceptions to this Policy

If the data owner determines that compliance with the provisions of this policy or any related information security policy would adversely impact a business process of the agency, the data owner may request approval to deviate from a specific requirement by submitting an exception request to the VSU Information Security Officer (ISO). For each exception, the requesting the data owner shall fully document:

1. The business need,
2. The scope and extent,
3. Mitigating safeguards,
4. Residual risks, and
5. The specific duration

Each request shall be in writing to the VSU ISO and approved by the VSU Chief Information Officer (CIO) indicating the acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception, as well as, mitigating controls and all residual risks. The requesting data owner will be informed of the action taken. An exception will not be accepted for processing unless all residual risks have been documented. Denied exceptions may be appealed to the CIO of VSU. The form to document exceptions requests is included in Attachment A of this document.

Once the exception request is approved by the VSU CIO, the request is then submitted to the Office of the President of VSU for signature and submitted to VITA Commonwealth Security and Risk Management Office for final approval by the COV CISO.

Policy Review

This policy will be reviewed every two years on the anniversary of the policy effective date or more frequently as needs of the University warrants.

Violations of Policy

1. Violation of this policy may result in:

a. Disciplinary action under the Virginia Department of Human Resources Policy 1.60, Standards of Conduct (4/16/08, 6/1/11).

b. Prosecution under "Virginia Computer Crimes Act." § 18.2-152.1.

c. Loss of Information Technology usage privileges.

References

Virginia Information Technology Agency (VITA):
Information Security Standard (SEC 501-09) (02/20/2015)

Library of Virginia Records Retention and Disposition Schedule for Administrative Records GS-101 located at: http://www.lva.virginia.gov/agencies/records/sched_state/GS-101.pdf

Library of Virginia Records Retention and Disposition Schedule for State Agencies: College and University located at: http://www.lva.virginia.gov/agencies/records/sched_state/GS-111.pdf

Approval By: _____ Date: 5/10/16
President

Title: Document Imaging Policy Policy: 6720