Document Retention and Destruction Policy

Section 1. PURPOSE AND SCOPE

This policy supplements and supports the Clark University Data Security Policies by defining the University's procedures for retaining and destroying documents containing any Confidential and/or Restricted data types as described in Clark University Data Classification Policies ("protected data".)

This policy describes procedures for compliance regarding the retention and the eventual destruction of protected data, and references a working spreadsheet (Clark University: Document Retention and Destruction Schedule) that lists specific documents that may or may not contain protected data. The Clark University: Document Retention and Destruction Schedule identifies the schedule for retention and destruction of each document type and may be a resource for future Discovery/eDiscovery proceedings.

Without adherence to these Document Retention and Destruction Policy standards, the University would be in a position of unnecessary reputational risk and financial liability. In the case of any litigation, Clark University may be required to produce documents for Discovery/eDiscovery. It is imperative that the University observe the retention and destruction practices and schedules established in this policy and in the Clark University: Document Retention and Destruction Schedule.

Who Should Read this Policy:

All administrative and academic department heads as well as third-party contractors should be aware of and comply with the policy.

Entities Affected by this Policy:

All Clark University departments (both administrative and academic) that handle, collect, maintain, access, or destroy documents that reside on paper or electronic media, must comply with the University's Document Retention and Destruction policy.

Third parties that process and/or store personal information for Clark, including, but not limited to:

- Digital fax/photocopier vendors and service providers
- Fundraisers
- Alumni relations service providers
- Student search providers
- Student account and/or payment/gift service providers (e.g. PayPal, CashNet, Authnet)
- File storage and backup management providers

- Document destruction service providers (e.g. shredding)

Section 2. PROCEDURES AND ENFORCEMENT

An obvious or deliberate breach of this, or any of Clark University's data security and confidentiality policies, is a serious infraction of University rules. The responsible party may be subject to disciplinary action, up to and including termination.

The Information Security Officer will oversee enforcement of the policy. Additionally, this individual will investigate any reported violations of this policy, lead investigations about data security breaches and may terminate access to protected information of any user who fails to comply with the policy. Other University Officers as needed and appropriate will assist the Information Security Officer.

Section 3. RETENTION AND DESTRUCTION

Retention and Access to Documents with Protected Data:

- All materials that contain, or may contain, protected data must be accounted for in the Clark University: Document Retention and Destruction Schedule by document type.
- Access to documents should be limited to only those individuals who have a business need to access them.
- Protected information not required to transact business (e.g. SSN) should be redacted (i.e. cut out or completely crossed out).
- Documents must be stored in a secure location, and must be destroyed before disposal via approved methods when retention is no longer required for business or legal purposes (retention period and/or date is specified in Clark University: Document Retention and Destruction Schedule).

Document Retention and Destruction Schedule:

- The Clark University: Document Retention and Destruction Schedule is published as a read-only document. The master copy is maintained by the Information Security Officer or designee.
- Information within this document is provided by managers, Data Managers and/or Data Custodians who retain protected data in any form.
- Required information includes the name of the responsible Data Manager/Custodian, the name of department, document type and description, and a specified date or specified length of time for retention that clearly identifies when retention of each document is no longer required.

- Retention date should be set based on when the document no longer needs to be retained for business or legal purposes.
- Retention date becomes the scheduled date for document destruction.
- Action taken may be "Destroy" (default) or "Move" (list other office/Data Manager/Custodian)
- It is the responsibility of the managers, Data Managers/Data Custodians to keep this information up to date by notifying the Information Security Officer or designee of any changes.
- It is the responsibility of the managers, Data Managers/Data Custodians to ensure that documents are retained and properly destroyed according to this policy and schedule.

Destruction of Documents with Protected Data:

- Documents may not be discarded until they are appropriately destroyed.
- Destruction must be via methods approved by Clark's Data Security Policies.
- Paper documents, CDs, DVDs, floppy disks and plastic identification cards to be destroyed should be deposited in secure containers provided by the University or destroyed locally in a crosscut shredder.
- Recorded media to be destroyed such as but not limited to USB keys, hard drives, and backup tapes should be brought to the ITS Help Desk so that it can securely destroyed or wiped for reuse.
- If using a shredder or method other than one that is specifically university-approved, contact the Information Security Officer for approval to use to ensure compliance with data security standards.

Section 4. DESTRUCTION DROP-OFF

Document Destruction Drop-Off Locations:

- Clark University will provide secure containers in several locations around campus for anyone to deposit paper documents to be properly destroyed (e.g. shredded) and disposed of by a University-approved facility. CDs, DVDs, floppy disks and plastic identification cards may also be disposed of in the secure shredding containers.
- Recorded media to be destroyed such as, but not limited to, USB keys, hard drives, and backup tapes should be brought to the ITS Help Desk so that it can securely destroyed or wiped for reuse.
- To locate the secure shredding bin closest to you, please contact the ITS Help Desk.

- To suggest another location for a secure container, or to express a question or concern over a current location, contact the Information Security Officer.

Section 5. PROCEDURES FOR COMPLIANCE

To achieve compliance with this policy, managers, Data Managers and/or Data Custodians are responsible to:

- Provide training on an ongoing basis to ensure all employees receive awareness and understanding of the current status of Clark's Data Security Polices and the importance of compliance.
- Identify documents currently used and/or retained within their domain, including usage and/or storage by third parties working within their purview.
- Review the required information in the Clark University: Document Retention and Destruction Schedule for each document that contains (or may contain) protected data.
- Destroy documents according to schedule.
- Communicate all changes (additions, changes, deletions and updates) as they occur to Information Security Officer and/or designee so they can update the master Clark University: Document Retention and Destruction Schedule document.
- Perform yearly self-assessments referencing the current data security policies, ensure required procedures are followed, and report compliance results.
- Return completed Document Retention and Destruction Self-Assessment Sign-off Form to Information Security Officer by July 1 each year which indicates that the self-assessment has taken place whether or not changes are required to the Clark University: Document Retention and Destruction Schedule.

Related Policies and Regulations

Data Security Policies
Document Retention and Destruction Schedule

History/Revision Information

Responsible Office/ Division: ITS

Effective Date October 27, 2010
Last Amended Date: June 23, 2015
Next Review Date: June 23, 2024