Data Security Policy for Supervisors, Data Managers and Data Custodians

Please also see the supporting documents:

- Data Classification Policy
- Data Security Definitions
- Data Access Policy

1. Clark University employees who have supervisory responsibilities and whose job responsibilities include the maintenance or use of Confidential data or Restricted data are responsible for ensuring compliance with Clark's data security policies as well as initiating corrective action if needed. In implementing these policies, each supervisory personnel is responsible for the following:
    - Communicating this policy to personnel under their supervision.
    - Ensuring that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect all University data.
    - Ensuring that employees under their supervision are properly trained in data management procedures.
    - Submitting an annual report to the Information Security Officer outlining departmental security practices and training participation
2. Electronic access to Confidential data should be granted by authenticating to a central Information Technology Services (ITS) resource. If it is not possible to use a central ITS authentication method, the application conducting the authentication must operate under the same policies as the central ITS resource (password and user lockout rules must apply and user accounts must be tied to a unique user).
3. Authorization for access to Confidential data or Restricted data shall be specified and approved by the respective Data Manager or Data Custodian, and must be made in conjunction with authorization or signed acknowledgement from the requestor, or other official authority.
4. When negotiating contracts with third party vendors, staff must consider whether such vendors require access to University databases or to other filing systems containing confidential information. Vendors should be contractually obligated to implement data protection and security measures that match the University's practices. If a vendor or consultant is to have access to Confidential data, the contract must be reviewed by the Information Security Officer to ensure the resulting contract has the following elements defined:
    - The contract must describe the purpose for access to the data.
    - Any Confidential data in transit electronically to the vendor must be encrypted.
    - Vendors /Consultants should be held accountable for the security and protection of any data that is in their possession.
    - Consultants must not disclose, allow access to, or permit other use of data beyond what is outlined within the contract.
    - Method of access to the data must be defined.

    No consultant or contractor is permitted to store Social Security number, driver's License number, credit or debit card number, state/federal ID card numbers, passport numbers, or

financial account numbers (checking, savings, brokerage, CD. . .) in any way relating to Clark or Clark-sponsored activities without the express written permission of Information Security Officer.

Created on: February 25, 2009
Last Reviewed: May 28, 2015

Authored by: VP for Information Technology and CIO
Reviewed by: Information Security Task Force
Approved by: Technology Steering Committee