Data Security Policy for All Faculty, Staff and Student Employees

Section 1. POLICY

- No member of the Clark community is permitted to electronically store or maintain credit card or debit card numbers, expiration dates, and/or security codes in any way relating to Clark or Clark-sponsored activities. Information Technology Services (ITS) must approve the use of any system or application that electronically processes, stores, or transmits credit card data.

  Paper documents containing credit card data should be secured in a locked office and stored in a cabinet. In an open office environment paper documents should be stored in locked cabinets. Paper documents should not be left in an unsecured office after work hours.

  All credit card processing (e.g., online, phone, mail, over-the-counter, card-swiping) must be reviewed and approved by the University Controller.

- The following confidential data types can only be electronically stored on an ITS managed server and can only be accessed from an ITS managed computer.
  - Social Security number
  - Driver's license number
  - State/Federal ID card number
  - Passport number
  - Financial account numbers (checking, savings, brokerage, CD...)

In the event that an exception is necessary in order to carry out the business of the University, the user must get written approval from both his/her Vice President as well as the Information Security Officer.

- It is recommended that all other Confidential data and restricted data types be electronically stored or accessed from the one of the following list of devices, in order of preference: ITS managed server, ITS managed desktop computer, encrypted laptop, encrypted mobile storage device. Any encrypted device must be encrypted using a process documented and approved by ITS and the administrator of such system must report to the Information Security Officer on system security related matters.

  When handling physical documents containing any Confidential and/or Restricted data types, the documents must be in your possession at all times; otherwise they should be stored in a secure location (e.g. room, file cabinet, etc.) to which only specifically-approved individuals have access through lock and key. When the information is no longer needed, the physical documents must be shredded using a university-approved device prior to being discarded; or destroyed by a university-approved facility.

Confidential data and Restricted data should not be taken or stored off-campus unless the user is specifically authorized to do so by a Vice President and notification of the authorization is sent to the Information Security Officer.

- Clark University reserves the right to electronically scan all Clark-owned resources and resources connected to the Clark network for Confidential data. In event that Confidential data is found in unauthorized locations, the Information Security Officer will follow-up with the responsible Vice President to remedy the situation.

- Confidential data cannot be transmitted through any electronic messaging (i.e. email, instant messaging, text messaging) even to other authorized users. Confidential data in a physical format cannot be transmitted through untracked delivery methods. Campus mail and regular postal services are not tracked delivery methods.

- All faculty, staff, and student Clark account passwords must be complex. A complex password is defined as follows:
  - At least eight characters long
  - Cannot contain three or more characters from the user's account name
    - Must contain 3 of the following categories
      - Uppercase English letter (A to Z)
      - Lowercase English letter (a to z)
      - Number 0 to 9
      - Non-alphanumeric character (!, #, $, & , =, etc…)
      - Unicode character

Clark account passwords will expire after 365 days. Passwords must never be written down or shared with other users.

- Users who are authorized to access or maintain Confidential data or Restricted data must ensure that it is protected to the extent required by Clark policy or law after they obtain it. All data users are expected to:
  - Access data only in their conduct of University business.
  - Request only the minimum Confidential data or Restricted data necessary to perform their University business.

- Respect the confidentiality and privacy of individuals whose records they may access.
- Observe any ethical restrictions that apply to data to which they have access.
- Know and abide by applicable laws or policies with respect to access, use, or disclosure of data.

Section 2. PROCEDURES AND ENFORCEMENT

Compliance with these data protection policies is the responsibility of all members of the University community. Violations of these policies will be dealt with seriously and will include sanctions, up to and including termination of employment. Users suspected of violating these policies may be temporarily denied access to the data as well as University information technology resources during investigation of an alleged abuse. Violations may also be subject to prosecution by state and federal authorities. Suspected violations of Clark's data protection policies must be reported to the Information Security Officer.

Related Policies and Regulations

Data Classification Policy

Data Security Definitions

Data Access Policy

History/Revision Information

Responsible Office/ Division:

Effective Date: February 25, 2009
Last Amended Date: May 28, 2015
Next Review Date: May 28, 2024