Clark University
Data Classification Policies
(http://www.clarku.edu/datasecurity)

	Confidential (highest, most sensitive)	Restricted (moderate level of sensitivity)	Public (low level of sensitivity)
Description	Data which is legally regulated; and data that would provide access to confidential or restricted information.	Data which the Data Managers have not decided to publish or make public; and data protected by contractual obligations.	Data which there is no expectation for privacy or confidentiality.
Legal Requirements	Protection of data is required by law.	Protection of data is at the discretion of the Data Manager or Data Custodian.	Protection of data is at the discretion of the Data Manager or Data Custodian.
Reputation Risk	High	Medium	Low
Data Access and Control	Legal, ethical, or other constraints prevent access without specific authorization. Data is accessible only to those individuals designated with approved access and signed non-disclosure agreements; and typically on a business "need to know" basis.	May be accessed by Clark employees and non-employees who have a business "need to know."	No access restrictions. Data is available for public access.
Transmission	Transmission of Confidential data through any non-Clark network or Clark guest network is prohibited (e.g. Internet). Transmission through any electronic messaging system (e-mail, instant messaging, text messaging) is also prohibited.	Transmission of Restricted data through any wireless network, and any non-Clark wired network is strongly discouraged. Where necessary, use of the University's VPN is required. Transmission through any electronic messaging system (e-mail, instant messaging, text messaging), is also strongly discouraged.	No other protection is required for public information; however, care should always be taken to use all University information appropriately.
Storage	Storage of Confidential data is prohibited on unauthorized Qualified Machines and Computing Equipment unless approved by the Information Security Officer. If approved, ITS approved encryption is required on mobile Computing Equipment. ITS approved security measures are also required if the data is not stored on a Qualified Machine. Storage of credit card data on any Computing Equipment is prohibited.	Level of required protection of Restricted data is either pursuant to Clark policy or at the discretion of the Data Manager or Data Custodian of the information. If appropriate level of protection is not known, check with Information Security Officer before storing Restricted data unencrypted.	No other protection is required for public information; however, care should always be taken to use all University information appropriately.
Documented Backup & Recovery Procedures	Documented backup and recovery procedures are required.	Documented backup and recovery procedures are not necessary, but strongly encouraged.	Documented backup and recovery procedures are not necessary, but strongly encouraged.
Documented Data Retention Policy	Documented data retention policy is required.	Documented data retention policy is required.	Documented data retention policy is not required, but strongly encouraged.
Audit Controls	Data Managers and Data Custodians with responsibility for Confidential data must actively monitor and review their systems and procedures for potential misuse and/or unauthorized access. They are also required to submit an annual report to the Information Security Officer outlining departmental security practices and training participation.	Data Managers and Data Custodians with responsibility for Restricted data must periodically monitor and review their systems and procedures for potential misuse and/or unauthorized access.	No audit controls are required.

Last Reviewed: July 2018

	Confidential (highest, most sensitive)	Restricted (moderate level of sensitivity)	Public (low level of sensitivity)
Data Examples (not all-inclusive) * exceptions apply	**Information resources with access to confidential or restricted data (username and password).** **Personally Identifiable Information (PII):** Last name, first name or initial with any one of following: - Social Security Number (SSN) - Driver's license - State ID card - Passport number - Financial account (checking, savings, brokerage, CD, etc .), credit card, or debit card numbers **Protected Health Information (PHI) *** - Health status - Healthcare treatment - Healthcare payment **Personal/Employee Data** - Worker's compensation or disability claims **Student Data not included in directory information. This includes:**** - Loan or scholarship information - Payment history - Student tuition bills - Student financial services information - Class lists or enrollment information - Transcripts; grade reports - Notes on class work - Disciplinary action - Athletics or department recruiting information **Business/Financial Data** - Credit card numbers with/without expiration dates * Exceptions apply ** Recent case law related to FERPA suggests that email containing information about a student's academic performance is not considered part of a student's "education record" unless the email is centrally maintained by the University (e.g., printed off and placed in the student's file). Clark suggests that faculty and staff be very mindful and attentive to the seriousness of the information being communicated about students as email is not a secure means of transmission.	**Personal/Employee/Student Data** - Clark ID number - Income information and payroll information * - Personnel records, performance reviews - Race, ethnicity, nationality, gender - Date and place of birth - Directory/contact information designated by the owner as private - ID card photographs for University use **Business/Financial Data** - Financial transactions which do not include confidential data - Information covered by non-disclosure agreements - Contracts that don't contain PII - Credit reports - Records on spending, borrowing, net worth **Academic / Research Information** - Library transactions - Unpublished research or research detail / results that are not confidential data - Private funding information - Human subject information - Course evaluations **Anonymous Donor Information** Last name, first name or initial (and/or name of organization if applicable) with any type of gift information (e.g., amount and purpose of commitment). **Other Donor Information** Last name, first name or initial (and/or name of organization if applicable) with any of the following: - Telephone/fax numbers, e-mail & employment information - Family information (spouse(s), partner, guardian, children, grandchildren, etc.) - Medical information **Management Data** - Detailed annual budget information - Conflict of Interest Disclosures - University's investment information **Systems/Log Data** - Server event logs	**Certain directory/contact information not designated by the owner as private**. - Name - Addresses (campus and home) - Email address - Listed telephone number(s) - Degrees, honors and awards - Most recent previous educational institution attended - Major field of study - Dates of current employment, position(s) Specific for students: - Class year - Participation in campus activities and sports - Weight and height (athletics) - Dates of attendance - Status **Business Data** - Campus maps - Job postings - List of publications (published research)