CARTHAGE
COLLEGE

Data Classification Framework

The Data Classification Framework was developed to aid users in appropriately protecting College data. The higher the classification level, the greater the required protection. Data must be consistently protected throughout its life cycle in a manner commensurate with its sensitivity and criticality. Policies regarding the storage and management of data, based on this *Data Classification Framework*, are outlined in the *IT Security & Acceptable Use of Technology* policy.

	Examples	Data at Rest	Data in Transit
Level 3 – Confidential / Restricted Data that is required to be protected by applicable law or statute (e.g., FERPA, HIPAA), or which, if disclosed to the public could expose the College to legal or financial obligations, or which the College has decided to keep confidential. It includes personally identifiable information which if disclosed would create risk of criminal liability, loss of insurability, severe social, reputational, or financial harm. In some cases, unauthorized disclosure or loss of this data would require the College to notify the affected individual and state or federal authorities and may.require informing the affected individual.	Examples: Social Security Numbers, Credit Card Numbers, Human Subjects Data, Academic records, health and medical records, personally identifiable information entrusted to our care, student financial aid information, disciplinary records, personnel records, applicant data, legally privileged information, information subject to a confidentiality agreement, alumni and donor information, course evaluations, financial budgets and plans, monthly financial management reports, unpublished financial information, HR performance plans and evaluations, customer data as defined by GLBA Note: Carthage has introduced service providers to handle credit card transactions, so no office should ever need to store credit card numbers.	Store only in Carthage enterprise applications, the S drive, or Google Team Drives under Carthage's G Suite for Education subscription, with access restricted. Applications must be protected by 2-factor authentication. If data has to live on your hard drive, your hard drive must be encrypted (using Bitlocker for Windows operating systems; orr Mac OS encryption) NOTE: LIS automatically encrypts hard drives for Carthage-owned computers issued to users	An email sent to an email domain that does not encrypt must be encrypted using FIPS 140-2 standards. Additional software licensing is required to perform this encryption, and available thru LIS. While Google itself meets the encryption requirements, emailing within Carthage.edu should be avoided by posting data to the appropriate data storage areas, due to the ease of forwarding and mishandling. LIS must encrypt sensitive interfaces
	Examples	Data at Rest	Data in Transit

Level 2 – Internal Information that would not cause material harm if disclosed, but is proprietary to the operation of the College, and should be made available to those with a need to know to perform their function effectively. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Internal info is not intended for public dissemination but may be released to external parties when there is a legitimate business purpose.	Definition: Information that would not cause material harm if disclosed, but is proprietary to the operation of the College, and should be made available to those with a need to know to perform their function effectively. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Internal information is not intended for public dissemination but may be released to external parties to the extent there is a legitimate business purpose.	Data should be maintained in Carthage enterprise applications or the S drive or Google Team Drives, with access only given based on appropriate role.	Email does not require FIPS 140-2 encryption LIS will put appropriate controls on interfaces
Level 1 – Public Carthage.edu external web site. Recruiting information, campus maps, building layouts, published information about the college, published research, course catalog, directory information about students who have not requested FERPA block, faculty and staff directory information	Examples: Carthage.edu external web site. Recruiting information, campus maps, building layouts, published information about the college, published research, course catalog, directory information about students who have not requested FERPA block, faculty and staff directory information	While the data can be freely shared, definitive master versions should be maintained in Carthage enterprise applications or the S drive or Google Team Drives. Update access to master versions still needs to be limited to appropriate parties.	No Email restrictions LIS will put appropriate controls on interfaces to prevent tampering

Revision History

Date	Description	Author

4/4/2022	Incorporation of revised FTC Safegurards Rule for customer information, consolidation of Level 3 and Level 4 since MFA has been enabled for Gsuite	M. Hobbins
7/29/2022	Annual Review	M. Hobbins