KECK GRADUATE INSTITUTE

A Member of The Claremont Colleges

Data Classification Standard

1. Introduction and Purpose

Keck Graduate Institute (KGI) Data Classification Standard provides specific instructions and requirements for classifying information assets. It also provides general data handling requirements for each of the specific classifications.

A data asset is defined as any data, or an aggregate of data, that has value to KGI and/or is used by KGI in support of business processes. This includes all electronic data (files, databases, etc.) and physical records (printed documents, etc.). Data assets include all information that must be protected to meet all applicable legislative, regulatory, and contractual obligations, including those under the Family Educational Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act (GLBA), as well as personal, private, or financial data about personnel, students, contractors, or other organizations.

2. Scope

All personnel, contractors, part-time and temporary workers, and those employed by others to perform work on KGI premises -- or who have been granted access to KGI information or systems -- are covered by this standard and must comply with associated guidelines and procedures.

This standard explicitly includes the following contexts and data environments:

- **Vendors and Contractors**: Any third-party service provider or contractor that processes or stores KGI data must comply with these standard and related data protection policies. Data handling of responsibilities must be clearly defined in contracts and service-level agreements (SLAs).
- **Cloud Service Providers (CSPs)**: All CSPs hosting KGI data must adhere to equivalent or stronger security controls, including encryption, identity management, and access auditing consistent with this policy.
- **Remote Work Scenarios**: Personnel accessing KGI systems remotely must use approved VPN and Multi-Factor Authentication (MFA). All devices, including [illegible]D, must comply with Mobile Device Management (MDM) requirements.
- **Mobile Access**: Data accessed through mobile devices must follow the Electronic Data Protections and BYOD standards outlined in Section 3.4.
- **Research Data**: Research data, including that governed by external grants (e.g., NIH, NSF, DoD), is subject to this policy. Such data must be classified at least as **Confidential** or **Restricted**, depending on sensitivity and sponsor requirements.

3. Definitions

PII (Personally Identifiable Information):
Information that identifies or can be used to identify an individual, such as name, address, date of birth, student ID, or other personal identifiers.

- **CUI (Controlled Unclassified Information):**

IRB (Institutional Review Board) Protected DataInformation requiring safeguarding under federal law or government contract but is not classified. CUI includes data governed by NIST 800-171 and federally funded research.

4. Requirements

4.1 Classifications and Data Management

KGI defines data classifications based on the sensitivity, criticality, confidentiality/privacy requirements, and value of the information. All information assets, whether generated internally or externally, must be categorized into one of the information classifications defined below. When information of various classifications is combined, the resulting collection of information or new information must be classified at the most restrictive level among the sources. Specific instructions and requirements for classifying information assets are provided in the Data Classification matrix below.

4.2 Categorization

	PUBLIC	INTERNAL	CONFIDENTIAL
Classification	1. Non-sensitive information available for external release, or 2. The loss of integrity, confidentiality, or availability of the data or system would have no adverse impact on KGI's mission, safety, finances, reputation, or on any individual.	1. Information that is only sensitive outside of KGI and is generally available to personnel and approved non-personnel, or 2. The loss of integrity, confidentiality, or availability of the data or system would have a mild to moderate adverse impact on KGI's mission, safety,	1. Information that is required to be protected by a law or regulation, or 2. The loss of integrity, confidentiality, or availability of the data or system would have a significant adverse impact on KGI's mission, safety, finances, reputation, or on any individual.

	e is no such thing as unauthorized disclosure of Public information.	finances, reputation, or on any individual. *Internal information should be limited to use within KGI and with its partners on a need-to-know basis. This is the default.*	*This information is intended for use by specific functional roles only.*
Examples	● KGI marketing or advertising literature once it is issued ● General product information ● Marketing brochures ● Job postings ● Approved press releases ● Information authorized to be posted on the KGI website	● Org Charts ● Personnel contact info ● Policies & Standards ● Procedure manuals ● Training materials ● Information intended for Public use but not yet released ● Information and materials intended for limited distribution ● Internal memos and emails, reports, budgets, plans, and financial information that does not contain Confidential data ● Contracts that do not contain Confidential data	● Accounting, financial, and tax information ● Technology and network schematics and information ● Encryption keys ● Strategic business and technology plans ● Vendor contracts containing Confidential data ● Controlled Unclassified Information (CUI) ● Student Education Records (FERPA) ● Student Identification Numbers (SID) ● Directory Information ● Financial Aid Applications (e.g. FAFSA) ● Financial Disbursement Data ● Institutional Financial Reports ● Account passwords ● PII ● Disciplinary records ● Salary & performance records ● All communications with Legal Counsel
Impact	● No adverse impact with unauthorized disclosure.	● Mild to moderate adverse impact with unauthorized disclosure.	Significant adverse impact with unauthorized disclosure: ● May result in substantial financial or legal liabilities ● May damage KGI's reputation ● May result in regulatory audit, oversight, or fines ● May result in criminal or civil litigation

4.2.1 Notes

1. **When Confidential information is combined with Internal or Public information,** the resulting collection of information must be classified as Confidential.
2. **When Internal information is combined with Public information**, the resulting collection of information must be classified, at a minimum, as Internal.
3. When information has **not been explicitly classified** as Confidential or Internal, the information shall **not** be considered Public by default.
4. Any information created or received by KGI personnel in the performance of their jobs at KGI is "Internal", by default, unless the information requires greater confidentiality or is approved for release to the public.

Treat information that is not assigned to a classification level as "Internal" at a minimum and use corresponding controls.

4.3 Access Control

	PUBLIC	INTERNAL	CONFIDENTIAL
Access Control	• Accessible to all personnel and non-personnel. • No access restrictions.	• Access is restricted to KGI personnel and approved non-personnel for business purposes only. • Access rights must be reviewed at least semi-annually and removed immediately upon employment termination, role change, or when no longer required for business purposes.	• Personnel access may only be granted with a documented business need-to-know and a documented supervisor for authorization. • Access by external parties requires an NDA as well as a documented business need-to-know. • Access may be granted to groups of authorized KGI personnel based on roles with a business need-to-know. • Strong 2FA is required for access, and access is logged and monitored. • Information must not be shown to or discussed with anyone without authorization. • Access to permissions must be documented, reviewed, and

			maintained according to KGI policies. - Exceptions may be granted for non-regulated data. NO exceptions may be granted for regulated data. - Access rights must be reviewed at least semi-annually and removed immediately upon employment termination, role change, or when no longer required for business purposes.

4.4 Electronic Data Protections

	PUBLIC	INTERNAL	CONFIDENTIAL
NDA	- No NDA requirements.	- An NDA is recommended prior to access by non-KGI personnel.	- An NDA is required prior to access by non-KGI personnel.
Storage	- No security control requirements.	- Local data storage access controls should be adequate to prevent casual disclosure. - Storage on privately owned platforms (BYOD) is prohibited unless explicitly authorized by IT.	- Information requires encryption unless explicit approval has been granted and documented. - Storage on privately owned platforms (BYOD) is prohibited unless specifically authorized, and the data files are encrypted. - All data types that are of a regulatory nature must be encrypted unless otherwise justified and documented.
Mobile Devices	- No security control requirements.	- Encryption is recommended. - Remote wipe should be enabled, if possible.	- Encryption is required. - Remote wipe must be enabled, if possible.

Removable Media	• The use of removable media (thumb drives) is discouraged. • Only encrypted thumb drives may be used.	• The use of removable media (thumb drives) is discouraged. • Only encrypted thumb drives may be used.	• The use of removable media (thumb drives) is not permitted unless explicitly authorized by IT.
Data at Rest (file servers, databases)	• Logical access controls are required to limit unauthorized use. • Physical access is restricted to specific groups.	• Encryption is recommended. • Logical access controls are required to limit unauthorized use. • Physical access is restricted to specific groups.	• Encryption is required. • Logical access controls are required to limit unauthorized use. • Physical access is restricted to specific individuals.
Disposal	• Removal of the directory entry for the file.	• Removal of the directory entry for the file.	• Use commercial overwrite software to destroy data. (A quick reformat of media is not sufficient.) • Physically destroy drives containing sensitive data.

4.4.1 Notes

1. BYOD (Bring Your Own Device) platforms include but are not limited to smartphones, privately owned flash storage devices, tablets, and all privately owned computers.

4.5 Physical Data Protections

	PUBLIC	INTERNAL	CONFIDENTIAL
Storage	● No security control requirements.	● Site and department storage should be adequate to prevent casual disclosure.	● Media must be kept in a locked drawer or equivalently secure environment. (See notes 1 & 2.) ● Media must be locked away when not physically in the presence of the originator. (See note 3.)
Printing	● No security control requirements.	● Verify the destination printer. ● Retrieve printed material without delay.	● Verify the destination printer. ● Attend to the printer while printing.
Fax	● No security control requirements.	● No security control requirements.	● Personally attend a receiving fax machine. ● Verify the destination number. ● Confirm receipt. ● Do not fax outside KGI without the manager's approval.
Disposal	● No security control requirements.	● Shred or delete all documents or place in a secure receptacle for future shredding. (There are shredders and Coro drop-boxes located in the facility.) ● Physically destroy electronic media or use commercial overwrite software.	● Shred or delete all documents or place in a secure receptacle for future shredding. (There are shredders and Coro drop-boxes located in the facility.) ● Physically destroy electronic media or use commercial overwrite software. (Quick reformatting of media is not sufficient.)

4.5.1 Notes

1. A secure environment is a physically secure area where written authorization is required to remove any physical information storage media (e.g., tapes, paper documents, optical disks, hard drives).

2. If any member of staff finds a Confidential item and it is not properly secured, it is their responsibility to secure it in accordance with the data classification assigned to it.
3. If any member of staff finds an item that is not actively used and is not stored securely, it is their responsibility to notify the business owner of that item for guidance on how to manage that item.

4.6 Data Labeling

	PUBLIC	INTERNAL	CONFIDENTIAL
Labeling of Documents	• No security control requirements.	• Documents must be labeled or watermarked as "Internal" • Documents containing CUI must be labeled.	• • Documents must be labeled or watermarked as "Confidential" • Documents containing CUI must be labeled. • Confidential physical documents that do not contain regulated data or CUI are exempt from labeling and watermarking requirements when retained within secured KGI facilities under controlled access.
Labeling of Media	• No security control requirements.	• No physical labeling is required.	• Physical labeling as CONFIDENTIAL is required for CUI or as required by law or regulations. • No physical labeling is required when in the KGI environment for non-regulated data.

4.7 Physical Distribution of Electronic Information

	PUBLIC	INTERNAL	CONFIDENTIAL
Distribution to Recipients	● No security control requirements.	● Distribution lists of those groups authorized to receive information must be checked regularly to ensure accuracy.	● Distribution is to named individual(s) only. ● The originator of the information item must keep a record of the unique identifier associated with the copy, and the named individual designated to receive that copy. ● The item may only be copied or distributed by the originator of the item. ● Items must be labeled with the classification before any copies are made.
Physical Mail	● No security control requirements.	● Envelopes must be sealed and tamper resistant. ● Envelope must show the recipient's name and address.	● Envelopes must be sealed and tamper resistant. ● Envelopes must show the recipient's name, address, and phone number. ● Envelopes must be marked "To Be Opened by Addressee Only".
Shipment Methods	● No security control requirements.	● Packaging should ensure physical protection of the item. ● Normal mail services may be used.	● Packaging must ensure physical protection of the item. ● Deliver by hand or approved courier. ○ <Add approved couriers.> ● Printed information sent by external mail must be sent by trusted courier or with Certified/ Registered mail. The method of mailing must provide tracking.

4.8 Transmission or Distribution of Electronic Information

	PUBLIC	INTERNAL	CONFIDENTIAL
Email	● No security control requirements.	● Use only **KGI-approved secure email or file transfer systems.**	● Use only **KGI-approved secure email or file transfer systems.** ● Do not forward emails or attachments. Instead, share via Box or One Drive with time-limited links and access restrictions.
Transmission (Internal)	● No security control requirements.	● Use only **KGI-approved secure email or file transfer systems.** ● Share files via Box or One Drive with time-limited links and access restrictions.	● Use only **KGI-approved secure email or file transfer systems.** ● Instant messaging is prohibited except through authorized services. ● Data transmitted by internal email must be flagged as "private" and "confidential" within the email system. ● Share via Box or One Drive with time-limited links and access restrictions.
Transmission (External)	● No security control requirements.	● Use only **KGI-approved secure email or file transfer systems**. ● Share files via Box or One Drive with time-limited links and access restrictions. ● End-to-end encryption is recommended. ● Instant messaging is prohibited except through authorized services. ● **Remote access requires VPN with MFA.**	● Use only **KGI-approved secure email or file transfer systems.** ● End-to-end encryption is required when transferred via public networks. Encryption can include either directly encrypting files or using secure file transport services. ● Instant messaging is prohibited except through authorized services. ● **Remote access requires VPN with MFA and is used only as necessary.** ● Share via Box or One Drive with time-limited links and access restrictions.

4.9 Remote Work / Off-Campus Transmission or Distribution of Electronic Information

		INTERNAL	CONFIDENTIAL
Transmission	● No security control requirements.	● Use only **KGI-approved secure email or file transfer systems.** ● Instant messaging is prohibited except through authorized services. ● **Remote access requires VPN with 2FA/MFA.**	● Use only **KGI-approved secure email or file transfer systems.** ● Instant messaging is prohibited except through authorized services. ● **Remote access should be used only when necessary and only with VPN and 2FA.**

4.10 Networking

	PUBLIC	INTERNAL	CONFIDENTIAL
Websites	● No security control requirements.	● Posting to publicly accessible Internet sites is prohibited. ● Posting to intranet sites is allowed.	● Posting to publicly accessible Internet sites is prohibited. ● Posting to intranet sites is prohibited unless pre-approved to contain Confidential data.
Video Calls	● No security control requirements.	● Confirm all participants on the call line.	● Confirm all participants on the call line. ● Ensure the call takes place in a private location.
Phone Calls	● No security control requirements.	● Pre-approve the roster of attendees. ● Confirm all participants on the call.	● Pre-approve the roster of attendees. ● Confirm all participants on the call. ● Ensure the call takes place in a private location. ●

4.11 Destruction / Reuse of Systems

	PUBLIC	INTERNAL	CONFIDENTIAL
Reuse of Workstations	● Workstation and laptops designated as only processing and storing “Public” data may be re-imaged and reused.	● Workstations and laptops designated as only processing and storing “Internal” and “Public” data may be re-imaged and reused.	● When workstations or laptops that may have processed or stored “Confidential” data are returned to the IT department, the position of the owner should be considered before issuing, wiping or re-imaging. ● If the owner was from a department that processes “Confidential” data, the hard drive should be overwritten with random bits multiple times and sanitized.
Servers and Networking	Servers and network equipment are not assumed to be Public.	● Media should be cleared of all institutional data before disposal	● When system and networking equipment reach end-of-life, they should be retired from production. ● Hard drives should be pulled and destroyed (for physical drives) or wiped (for virtual drives). ● Full drive encryption should be employed on mobile systems, where feasible. ● Disposal should be documented. Certificates of destruction should be provided by third parties.

5. Data Classification Examples

The following are examples of how data is typically classified. Be aware that **data, when combined with other data, may increase sensitivity and handling requirements.** If you are uncertain how to handle any piece of information, contact the KGI IT Service Desk at helpdesk@kgi.edu for guidance from the ISO.

5.1 Table of Examples

Data Class	Sensitive Data Elements	Public	Internal	Confidential
Student or Personnel-Related Personal Data	Social Security Number (SSN)			X
	Employer Identification Number (EIN)			X
	Student Identification Numbers (SID)			X
	Driver’s License (DL) Number			X
	Financial Account Number			X
	Controlled Unclassified Information (CUI)			X
	Student Education Records			X
	Directory Information			X
	Financial Aid Applications (e.g. FAFSA)			X
	Financial Disbursement Data			X
	Institutional Financial Reports			X
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)			X
	Immigration Status			X
	Birth Date			X
	First & Last Name		X	
	Age		X	
	Phone and/or Fax Number		X	
	Home Address		X	
	Gender		X	
	Ethnicity		X	
	Email Address		X	
	Compensation & Benefits Data			X

	Medical Data			X
	Workers Compensation Claim Data			X
	Education Data			X
	Dependent or Beneficiary Data			X
Sales & Marketing Data	Business Plan (including marketing strategy)			X
	Financial Data Related to Revenue Generation			X
	Marketing Promotions Development		X	
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions)	X		
	News Releases	X		
Network & Infrastructure Data	Username & Password Pairs			X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)			X
	Hardware or Software Tokens (multi-factor authentication)			X
	System Configuration Settings			X
	Regulatory Compliance Data			X
	Internal IP Addresses			X
	Privileged Account Usernames			X
	Service Provider Account Numbers			X
	Summary results of Penetration Tests & other Security Assessments			X
	Detailed results of Penetration Tests & other Security Assessments			X
Strategic Financial Data	Corporate Tax Return Information			X
	Legal Billings			X
	Budget-Related Data			X
	Unannounced Merger and Acquisition Information			X
	Trade Secrets (e.g., design diagrams, competitive information)			X
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X
	Paychecks			X
	Incentives or Bonuses (amounts or percentages)			X
	Stock Dividend Information			X
	Bank Account Information			X
	Investment-Related Activity			X
	Account Information (e.g., stocks, bonds, mutual funds, money markets)			X
	Debt Amount Information			X

5.1.1 Personally Identifiable Information (PII)/Personal Data

Personally Identifiable Information (PII) is any information that can be used to identify, contact, or locate a specific individual, either by itself or when combined with other information. **Examples include**, but are not limited to:

- **Names and Identifiers**
  - Full name, or first name/initial plus last name
  - Alias or maiden name
- **Government-Issued Numbers**
  - Social Security Number (SSN), Taxpayer Identification Number (TIN), National Identification Number (NIN)
  - Passport number
  - Driver’s license or state ID number
  - Permanent resident card number
- **Financial Information**
  - Bank account number
  - Credit or debit card number
  - Financial transaction or disbursement details
- **Other Identifying Information**
  - Date and place of birth
  - Home or email address
  - Telephone number
  - Student or employee ID number
  - Medical record number
  - Biometric identifiers (e.g. fingerprint, facial image, voiceprint, iris scan)
  - Geolocation data (e.g. precise GPS)

5.1.2 Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is unclassified information the United States Government creates or possesses that requires safeguarding or dissemination controls limiting its distribution to those with a lawful government purpose. CUI may not be released to the public absent further review. CUI possessed and maintained by KGI has been identified as:

- Financial Aid Applications (e.g. FAFSA)
- Financial Disbursement Data
- Institutional Financial Reports
- Student Identification Numbers
- Pre-publication Data from Federally Sponsored Research

6. Roles and Responsibilities

The Information Security Officer (ISO) is responsible for ensuring the development, implementation, and maintenance of the Data Classification Standard. The ISO ensures consistent application of data protection standards across the institution. When disputes emerge, the ISO will work with KGI's legal team to provide final determinations.

KGI management, including senior management and department managers, is accountable for ensuring that the Data Classification Standard is properly communicated and understood within its respective organizational units. KGI management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the Data Classification Standard.

Role	Description
Control Owner	IT Director
Information Security Officer (ISO)	IT Director
Asset Owners (Owners)	Accountable for safeguarding information within their area, defining and maintaining classification and handling processes, coordinating with the Information Security Program, and ensuring systems and data under their authority remain accurate and compliant.
Asset Custodians (Custodians)	Responsible for securely managing and maintaining information systems on behalf of Data Owners, ensuring proper configuration, documentation, and operation while upholding confidentiality, integrity, and availability. They coordinate with the Information Security Program to maintain compliance and security across KGI environments.

6.1 Asset Owners (Owners)

These are the managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the ISO will make the designation. The Owner is responsible for defining processes and procedures that are consistent with the Data Classification Standard, coordinating with the Information Security Program (ISP) to ensure that organizational protection standards are properly established and maintained, and ensuring that accurate and updated information on network devices and servers in the production environment is retained.

6.2 Asset Custodians (Custodians)

These are the managers, administrators, and those designated by the Owner to manage, process, or store information assets. Custodians are responsible for maintaining a secure processing environment that protects the confidentiality, integrity, and availability of information; coordinating with the ISP Program to ensure KGI’s security requirements are properly established and maintained; configuring network devices, servers, and desktop systems in production environments in accordance with institutional security standards; retaining and updating accurate information on network devices and servers in the production environment; and cooperating with the Information Security Program in efforts to verify compliance across production systems.

6.3 Users

These are the individuals, groups, or organizations authorized by the Owner to access information assets. Users are responsible for familiarizing themselves and complying with the Data Classification Standard and associated guidelines, following KGI-approved processes and procedures to request authorization to install hardware or software on their desktop or mobile system, ensuring desktop and mobile systems are available for automated updates, and maintaining the confidentiality, integrity and availability of information accessed, consistent with the Owner’s approved safeguards while under the User’s control.

7. Enforcement and Exception Handling

Failure to comply with the Data Classification Standard and associated guidelines and procedures can result in disciplinary actions up to and including termination of employment for personnel or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the Data Classification Standard should be submitted to the IT service desk at **helpdesk@kgi.edu**. Exceptions are granted only with written approval from the ISO, who will consult with Legal as needed for final determination in the event of a disagreement.

- **Periodic Audits**: The ISO will conduct **annual audits** and **spot checks** to assess adherence to the Data Classification Standard.

- **Reporting**: Audit results will be reported to senior management, and remediation plans are implemented.
- **Automated Monitoring**: Where feasible, automated tools (e.g., DLP, access reviews, and system logs) will be used to detect policy violations or control failures.

8. Aligned Governance Documents

8.1 Aligned Sections of the ISP

- [ISP sections 13.1, 25.2, 25.3, 25.4, 25.5]

8.2 Aligned Standards

- 11.6.2 Data Protection Standard
- 26.9.1 Data Retention Standard

8.3 Aligned Procedures

- N/A

9. Compliance

All relevant legislative statutory, regulatory, and contractual requirements and KGI's approach to meeting these requirements are explicitly identified, documented, and kept up to date.

10. Document Control

Document Name	13.1.1 Data Classification Standard
Classification	**Confidential**
Distribution	**Access Limited to Authorized Personnel**

11. Approval

Role	Name	Approval Date
CFO	Trevor Garrett	12/15/2025

12. Change History and Revision Control

Version	Sections Revised	Description	Changed By	Date
1.0	All	Document review, final draft	Rick Burgess	10/25/2025
1.1		Review and formatting updates	Rick Burgess	12/15/2025