Data Management and Protection Training
Learning Objectives

• Learn to identify (inventory), classify (categorize) and safeguard the Data in your custody.
• Review policies and procedures governing University Data
• Feel confident that you can apply the appropriate controls for protecting data, from the point of collection, to storage, transmission, to archiving and/or destruction.
What is Data Management?

Data management is the practice of collecting, keeping, and using data securely, efficiently, and cost-effectively.

The goal of data management is to help people and organizations optimize the use of data within the bounds of policy and regulation.
**Data**: pieces of information, which can exist in a variety of forms.

Examples of data:
- Personal data (name, SSN, DL, address, health information, etc.)
- Health data
- Financial data (credit card, bank info)
- Facilities data (campus map, buildings, addresses, parking info, emergency phones, etc.)

**Record**: Any kind of documented evidence of an activity or transaction.

Records are “snapshots” of data, at a particular time, for a particular **purpose**.

Examples of Records:
- Student admission forms
- Correspondence (Memoranda, Letters, E-mails)
- Data files, Reports, Meeting minutes

"Records contain Data."
Privacy Laws and Regulations - examples

**FERPA** - Under the [Family Educational Rights and Privacy Act](https://en.wikipedia.org/wiki/Family_Educational_Rights_and_Privacy_Act) of 1974, the university is required to protect the privacy of students' personally identifiable information (PII).

**GLBA** - the [Gramm-Leach-Bliley Act](https://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.

**GDPR** - the [General Data Protection Regulation](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation) is a regulation in EU law, which protects the privacy of European Union’s (EU) residents' personal data.

**HIPAA** - the [Health Insurance Portability and Accountability Act](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act) (HIPAA) is a Federal law that requires the protection and confidential handling of protected health information.

**PCI DSS** - The [Payment Card Industry Data Security Standard](https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard) is an information security standard created to increase controls around cardholder data, to reduce credit card fraud.

**SSN** – State Laws regulating, restricting or prohibiting the collection, use or disclosure of an individual’s Social Security number (“SSN”) by commercial entities.
GW Policies governing University Data

The **Personal Information and Privacy Policy**, **Records Management Policy**, and the **Information Security Policy** require that we manage and protect university data based on its level of sensitivity, value and criticality to the university.

**Social Security Number and GWID Usage Policy** - All university departments must use the GWid as the primary Identifier for all university purposes. When use of the SSN is required, departments must protect the confidentiality of SSN data, regardless of format.

**Payment Card Acceptance and Data Security** - Credit and debit cardholder data is regulated data that must be appropriately secured. The university is required to be compliant with the Payment Card Industry Data Security Standards (PCI DSS).

**GW Privacy of Student Records Policy** - The university and its faculty and staff will protect the privacy of students’ education records as required by federal law and regulations.

**GW Health Information Privacy Policy** - The GW University Health and Welfare Benefit Plan is committed to and takes reasonable steps towards protecting the privacy of employees’ Protected Health Information (“PHI”).
Data management begins with the creation or collection of data and continues through the entire data lifecycle.

- **Data Collection**
  - Collect only what is relevant to the purpose

- **Storage**
  - Secure storage

- **Use (processing)**
  - Purpose
  - Who is accessing it?

- **Transmission**
  - Security when data is in transit (Encryption)

- **Archiving** (long term storage)
  - Legal basis;
  - retention requirements

- **Data destruction**
  - Is it really gone?
Data Management and Protection Standard

The Data Management and Protection Standard is a framework for classifying university data, based on its level of sensitivity, value and criticality to the university, and protecting it as required by the Personal Information and Privacy Policy, Records Management Policy, and the Information Security Policy.

This Standard applies to students, faculty, staff, contractors, and any persons or entities who generate, collect, use, store, or process personal information on behalf of the University.

Data management begins with the creation or collection of data and continues through the entire data lifecycle. As such, data management consists of the following main phases:

1. Data Inventory
2. Data Classification
3. Data Protection
4. Report Regulated data

Data Inventory

A data inventory is a detailed record of the data maintained by the university (“university data”). The data inventory process consists of identifying and recording basic information about data in your custody, such as: data owner, data format, record category and retention requirement (per the University Records Schedule), storage, access, transfer, purpose of processing, etc.

The Data Inventory Template (xlsx) should be used to capture all relevant information about your data.

A data inventory is valuable because it provides information on what data you have, where it’s located and
Data inventory provides information on what data you have, where it’s located and who has access to it.

Data Inventory also helps identify information that must be safeguarded under requirements of laws (e.g. FERPA, HIPAA, GLBA), regulations (GDPR), industry standards (PCI DSS) and university requirements and policies.

Review your data inventory on a periodic basis to determine if there have been any material changes, such as changes to a record category, storage location or access to data that is in the custody of that unit.

For assistance with completing or reviewing your data inventory, contact Privacy@gwu.edu.
Data Inventory Template

For assistance with completing or reviewing your data inventory, contact Privacy@gwu.edu.
Data Classification helps identifying the level of privacy and security protection to be applied to University Data (and records) and the scope and means in which the data/records can be shared.

**PUBLIC**
- Low risk
- Little or no controls are required to protect the confidentiality of Public data, yet, some level of control is required to prevent unauthorized modification or destruction of it.
- Open Access

**Examples:**
- Announcements / press releases
- Public event information
- Public directories and maps;

**RESTRICTED**
- Moderate risk
- Must be protected from unauthorized access, use or disclosure due to university policies, contract, or designation, or due to proprietary or privacy considerations.

**Examples:**
- Course information / schedules;
- Access codes, legal records and contracts; general ledger data;
- Facilities records

**REGULATED**
- High risk
- Must be protected from unauthorized access, use or disclosure due to university policies, contract, or designation, or due to proprietary or privacy considerations.

**Examples:**
- Student academic records;
- Protected Health Information;
- Personal Identifiable Information (e.g. SSN, DL, DoB)

**GW Guide for Data Classification**
# Data Classification

Example of common Data Types accompanied by the corresponding Data Classification.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description &amp; Examples</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private Personal Information / Personally Identifiable Information (PII)</strong></td>
<td>This is a category of sensitive information that is associated with an individual person (e.g., employee, student, etc.)</td>
<td>REGULATED</td>
</tr>
<tr>
<td>• Social Security number</td>
<td>□ Biometric information</td>
<td></td>
</tr>
<tr>
<td>• Individual Tax IDs</td>
<td>□ Biographic/demographic data (Date and location of birth, Country of citizenship, Citizenship status, Marital status, Military status)</td>
<td></td>
</tr>
<tr>
<td>• National ID number</td>
<td>□ Criminal record &amp; criminal background check information</td>
<td></td>
</tr>
<tr>
<td>• Passport number</td>
<td>□ Tax information (e.g., W-2, W-4, 1099)</td>
<td></td>
</tr>
<tr>
<td>• Visa permit number</td>
<td>□ Disciplinary information</td>
<td></td>
</tr>
<tr>
<td>• Driver’s license number</td>
<td>□ Leave-of-absence reason</td>
<td></td>
</tr>
<tr>
<td>• Bank and credit/debit card numbers</td>
<td>□ Payroll and benefits information security</td>
<td></td>
</tr>
<tr>
<td>• Disability information</td>
<td>□ Health information</td>
<td></td>
</tr>
<tr>
<td>• Ethnicity, Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Financial account number in combination with a code, access code or password that would permit access to the account</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Protected Health Information (PHI)** | The following individually identifiable data elements, when combined with health information about that person, make such information protected health information (PHI): | REGULATED |
| Name | □ Social Security number |
| Telephone number | □ Medical record number |
| Fax number | □ Health plan beneficiary number |
| Email address | □ Certificate/license number |
| Address (all geographic subdivisions smaller than including street county, zip code) | □ Vehicle identifier and serial number, including license plate number |
| Internet protocol (IP) | □ Device identifier and serial number |
| | □ Universal Resource Locators (URLs) |
| | □ Biometric identifier, including finger and voice print |
| | □ Any other unique identifying state number, characteristic, address, city, code, or combination that precipitates or allows identification of an individual addresses |
## Data Classification

Example of common Data Types accompanied by the corresponding Data Classification.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description &amp; Examples</th>
<th>Classification</th>
</tr>
</thead>
</table>
| **Payment Card Industry (PCI) Information** | Information related to credit, debit, or other payment cards. This data type is governed by the Payment Card Industry (PCI) Data Security Standards. Credit or debit card numbers cannot be stored in any electronic format. (If someone can override this, add who can do it and through which process)  
  - Cardholder name, Service code, PIN or PIN block  
  - Credit/Debit card account number  
  - Credit/Debit card expiration date  
  - Credit/Debit card verification number  
  - Credit/Debit card security code (CVC2, CVV2 or CID value)  
  - Credit/Debit card’s magnetic stripe content.                                                                                                                                                                                                                      | REGULATED       |
| **Personal Data from European Union (EU)** | The EU’s General Data Protection Regulation (GDPR) defines personal data as any information that can identify a natural person, directly or indirectly, by reference to an identifier including  
  - Name  
  - Any identification number  
  - Location data  
  - An online identifier  
  - One or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person  
  Any personal data that is collected from individuals in European Economic Area (EEA) countries is subject to GDPR.                                                                                                                                                            | REGULATED       |
| **Student Education Records (FERPA)** | Records that contain information directly related to a student and that are maintained by the University or by a person acting for the University. The Family Educational Rights and Privacy Act (FERPA) governs release of, and access to, student education records. “Directory information” about a student is not regulated by FERPA and can be released by the University without the student’s permission. Students can request non-disclosure from the Registrar’s Office.                         | REGULATED       |
Data Classification

Example of common Data Types accompanied by the corresponding Data Classification.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description and Examples</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Loan Application Information</td>
<td>Personal financial information held by financial institutions and higher education organizations as related to student loan and financial aid applications. Gramm Leach Bliley Act (GLBA) provisions govern this data type.</td>
<td>REGULATED</td>
</tr>
<tr>
<td>Federal Tax Information</td>
<td>FTI is defined as any return, return information or taxpayer return information that is entrusted to the University by the Internal Revenue Services. See <a href="https://www.irs.gov/individuals/internal-revenue-service-publication-1075-exhibit-2">Internal Revenue Service Publication 1075 Exhibit 2</a> for more information.</td>
<td>RESTRICTED</td>
</tr>
<tr>
<td>Contractual Non-Disclosure</td>
<td>Information, materials, data, and records designated confidential by contract, including information obtained by the University from third parties under non-disclosure agreements or any other contract that designates third party information as confidential.</td>
<td>RESTRICTED</td>
</tr>
<tr>
<td>Departmental Administration</td>
<td>Budgetary, departmental, or University planning information. Non-public financial, procurement, health/safety, audit, insurance and claims information.</td>
<td>RESTRICTED</td>
</tr>
</tbody>
</table>
### Computing Equipment

<table>
<thead>
<tr>
<th>Information Category</th>
<th>Regulated</th>
<th>Restricted</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Category</strong></td>
<td>High Risk</td>
<td>Moderate Risk</td>
<td>Low Risk</td>
</tr>
</tbody>
</table>

#### Laptops and Mobile Devices - GW-owned or approved

**(Desktop, laptop, phone, tablet)**

- Regulated Data should only be accessed and processed with GW-owned or approved computers or mobile devices (such devices are configured and managed by the university and must be encrypted).
- Devices used to access and process Regulated data should be registered and managed by GW IT.

#### Personally-Owned Devices

***(Desktop, laptop, phone, tablet)***

- **Regulated or Restricted information may not be downloaded, stored or synchronized on personally-owned workstations or mobile devices.**

Requirements for **accessing Regulated Information** from personally-owned workstations or mobile devices are:
- Full Disk Encryption (FDE)
- **Use of VPN**
- Must be password protected
- Anti-Virus / Anti-Spyware software must be active and maintained up to date (Symantec Endpoint Protection available from it.gwu.edu download page)
- Updates for all installed software, as well as firmware and driver updates should be installed within a reasonable period.

Contact your IT Department and/or GW Information Security for further instructions.

### Contact your IT Department and/or GW Information Security for further instructions.
# Data Protection

<table>
<thead>
<tr>
<th>Information Category</th>
<th>Regulated</th>
<th>Restricted</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Category</td>
<td>High Risk</td>
<td>Moderate Risk</td>
<td>Low Risk</td>
</tr>
</tbody>
</table>

## STORAGE

### Storage

<table>
<thead>
<tr>
<th>Regulated data in physical form (paper, media) should be locked at all times and access should be restricted only to authorized users, with a legitimate business need.</th>
</tr>
</thead>
<tbody>
<tr>
<td>May be stored on departmental, GW IT-hosted, or approved cloud-based systems.</td>
</tr>
<tr>
<td>May be stored in the following GW systems: GW G-Drive, GW SharePoint, GW Box and GW Docs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Restricted data in physical form (paper, media) should be secured at all times and access should be restricted only to authorized users, with a legitimate business need.</th>
</tr>
</thead>
<tbody>
<tr>
<td>May be stored on departmental, GW IT-hosted, or approved cloud-based systems.</td>
</tr>
<tr>
<td>May be stored in the following GW systems: GW G-Drive, GW SharePoint, GW Box and GW Docs.</td>
</tr>
</tbody>
</table>

Contact your IT Department and/or GW Information Security for further instructions.
# Data Protection

<table>
<thead>
<tr>
<th>Information Category</th>
<th>Regulated</th>
<th>Restricted</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Category</td>
<td>High Risk</td>
<td>Moderate Risk</td>
<td>Low Risk</td>
</tr>
</tbody>
</table>

## TRANSMISSION

<table>
<thead>
<tr>
<th>Emailing</th>
<th>Avoid emailing regulated data.</th>
<th>Avoid emailing restricted data.</th>
<th>No limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If there is a legitimate business need to email regulated data, it must be encrypted during transmission and VPN must be used.</td>
<td>If there is a legitimate business need to email restricted data, it must be encrypted during transmission and VPN must be used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emailing Regulated Information to or from a personal email address is strictly prohibited.</td>
<td>Emailing Restricted Information to or from a personal email address is discouraged.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contact your IT Department and/or GW Information Security for further instructions.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## PRINTING or Reproduction

<table>
<thead>
<tr>
<th>Printing and Reproduction (copy)</th>
<th>Avoid printing regulated data.</th>
<th>Avoid printing restricted data.</th>
<th>No limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Regulated Data should never be printed on any public device.</td>
<td>Restricted Data should never be printed on any public device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The minimum necessary prints / copies may be made only by permission of originator or his/her designates. Working copies (prints) containing regulated data should secured at all times and returned to office or permanently destroyed (shredded) when no longer needed.</td>
<td>Only the minimum necessary copies (prints) should be made. Working copies containing restricted data in should secured at all times and returned to office or permanently destroyed (shredded) when no longer needed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contact <a href="mailto:Privacy@gwu.edu">Privacy@gwu.edu</a> for further guidance.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Guidance

As a general rule, regulated or restricted data should not be exported into spreadsheets or inserted into emails, instant messages or other forms of transmission. Data should remain in the enterprise systems or applications where it can be securely managed.

Use of computing equipment (Laptops, mobile devices)
Use your GW managed devices for University business.
*If you do not have a GW managed device, you should not download or store data on your personally owned computer or mobile device.*

Emailing
Data should not be emailed in an attachment, instead, use GW Box links or share via Google drive. Personal email should not be used for conducting GW business.

Printing, Copying and Scanning
Data should not be printed or scanned on any public device. Make only the minimum necessary prints/copies. Protect copies from unauthorized access or misuse. When no longer needed, copies should be shredded, either at telework location if possible, or held in a secure manner for shredding at GW upon return to normal operations.
Data Protection

Virtual Meeting Applications (Guidance)

- Use only virtual tools and technologies that have university approved contracts.
- To protect restricted and regulated data, virtual tools and technologies should be integrated with **GW Single-Sign On** or **two-factor authentication** as well as have the capability for event-specific **password protection, encryption and attendance control**.
- Use a **non-public meeting room** if your virtual event will contain any sensitive content and/or personal identifiable information (PII or PHI).
  - One-time password or access code for entry into the meeting room is required; End to end encryption is strongly recommended. All available encryption and privacy modes should always be enabled
- **Do not record the virtual meeting unless it’s absolutely necessary.**
- If the content will not include any personal identifiable information (deidentified PII or PHI or general administrative or academic content), a **public meeting room** can be used.
  - **For example, a WebEx personal room is a public meeting room unless a password has been enabled.**
- Before anyone shares their screen, files or other content, remind them not to share sensitive or personally identifiable information during the meeting inadvertently.
To report a data incident involving Non-Public Information or a suspected data breach, email incident@gwu.edu and privacy@gwu.edu or use the reporting form on the privacy website.

Data incident examples:
- Accidental data disclosure
- Loss / theft of device storing university data
- Computer system breach
- Hacking; malware, spyware
- System access issues
- Unauthorized access of protected information by insider, with malicious intent
Report REGULATED data to the Privacy Office

Per the Personal Information and Privacy Policy, data custodians must report to the Privacy Office (privacy@gwu.edu) if they have any regulated data in their custody.

Examples:

- Government-issued identification numbers, including social security numbers, driver license numbers, and passport numbers.
- Financial account numbers, including credit card numbers and bank account numbers.
- Personal health or medical information.
- Data, information, or technical specifications not in the public domain that are regulated by export control laws, excluding technology or software that arises during, or results from, fundamental research under Section 734.8 of the Export Administration Regulations (EAR).
Questions?
Contact:

PRIVACY@gwu.edu