Explore Tools & Services
Tools & Services by Category
Administrative and Business
Business Capability and Process Automation
Data, Reporting, and Analytics
Data Management
Business Intelligence Services
Data Integration
Data Lake
Data Governance
Data & Reporting
Institutional Data
Data Governance Center
Data Classification & Protection
Data Classification Guide
Data Protection Guide
Data Quality
Data Stewardship
Data Sharing
Data Awareness
Financial and Procurement Systems
Human Resource Systems
Student Information Systems
Communication and Collaboration
Desktop and Mobile Computing
IT Professional Services
Information Security
Infrastructure

Data Protection Guide

Protecting GW institutional data from unauthorized access or use is critical to maintaining the confidentiality, integrity, and availability of all data stored, processed, printed, and/or transmitted by faculty, staff and, where applicable, third parties. Throughout its lifecycle, institutional data must be protected in a manner that is consistent with contractual or legal requirements. Additionally, data protection measures must be reasonable and appropriate for the classification level. For example, a document that contains regulated and public information must be managed and protected in accordance with requirements for regulated information.

This guide outlines data protection measures for GW Institutional data. When procuring software or third-party services that will involve access to or use of institutional data, Faculty and Staff are required to follow GW's Procurement process to ensure compliance with GW privacy and security protocols.

View Physical Security Best Practices.

Data Category	**Regulated**	**Restricted**	**Public**
Risk Level	High Risk	Medium Risk	Low Risk
Network	All network traffic must be encrypted in transit using at least TLS v1.1.(TLS v1.2 is strongly encouraged). It's always preferable to use the strongest cipher available when transmitting Regulated Information, especially when transmitting to a third party.	All network traffic must be encrypted in transit using at least TLS v1.1.(TLS v1.2 is strongly encouraged).	No limitations
Workstations or Mobile Devices - GW-owned or approved (Desktop, laptop, phone, tablet)	Regulated data may be accessed and processed using GW-owned or approved workstations or mobile devices (such devices are configured and managed by the university and must be encrypted). The following security controls must be in place: • Strong Password • Encryption • Remote wiping capability • Registered and managed by the GW IT mobile device management service.	Restricted data may be be accessed and processed using GW owned or approved workstations or mobile devices (such devices are configured and managed by the university and must be encrypted). The following security controls must be in place: • Strong Password • Encryption • Remote wiping capability • Registered and managed by the GW IT mobile device management service.	No limitations

- Research
- Teaching and Learning
- For Faculty
- For Staff
- For Students
- For Researchers
- For Alumni
- For Affiliates
- For Visitors

Data Category **Risk Level**	**Regulated** High Risk	**Restricted** Medium Risk	**Public** Low Risk
Personally Owned Devices (Desktop, laptop, phone, tablet)	Regulated information may not be downloaded, stored or synchronized on personally owned workstations or mobile devices. GW Storage systems approved for regulated information may be accessed but not installed. Requirements for accessing regulated Information from personally owned workstations or mobile devices are: • Full Disk Encryption (FDE) • Use of VPN (Use the GW VPN when working remotely and accessing regulated data.) • Must be password protected • Anti-Virus / Anti-Spyware software must be active and maintained up to date • Updates for all installed software should be installed within a reasonable period • Firmware and driver updates should be installed within a reasonable period	Restricted information may not be downloaded, stored or synchronized on personally owned workstations or mobile devices. GW Storage systems approved for restricted information may be accessed but not installed. Requirements for accessing restricted information from personally owned workstations or mobile devices are: • Full Disk Encryption (FDE) • Use of VPN (Use the GW VPN when working remotely and accessing restricted data.) • Must be password protected • Anti-Virus / Anti-Spyware software must be active and maintained up to date • Updates for all installed software should be installed within a reasonable period • Firmware and driver updates should be installed within a reasonable period	No limitations

Data Category	**Regulated**	**Restricted**	**Public**
Risk Level	High Risk	Medium Risk	Low Risk
Storage	Regulated information may be stored only on GW IT hosted or approved servers or services (such as file sharing or collaboration services, cloud- based services, cloud-based back-up and recovery services, etc.) Documents containing regulated data may be stored in the following GW systems: • GW Box • GW Documents (Documentum) Never store regulated information on laptops or mobile devices, including USB and external hard drives. Regulated data in physical form (paper, media) should be secured (locked) at all times and access should be restricted only to authorized users, with a legitimate business need.	Restricted data may be stored on departmental, GW IT hosted or approved cloud-based systems. Documents containing restricted Data may be stored in the following GW systems: • GW Box • GW Google Drive • GW SharePoint • GW MS Teams • GW Documents (Documentum) 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.	No limitations
Access	Access to regulated data must be limited to only authorized individuals (staff, faculty), who have a legitimate reason to access it (on a business "need to know" basis). Data Custodians are responsible for all access and permissions to regulated data in their custody. Data Custodians must: • Determine who needs access to the regulated data in their custody and what permission level needed for each individual. • Follow the Principle of Least Privilege: give individuals the lowest permission levels needed to perform their assigned tasks. • Periodically review access to the	Access to restricted data must be limited to only authorized individuals (staff, faculty), who have a legitimate reason to access it. Data Custodians are responsible for all access and permissions to restricted data in their custody. Data Custodians must: • Determine who needs access to the restricted data in their custody and what permission level needed for each individual. • Follow the Principle of Least Privilege: give individuals the lowest permission levels needed to perform their assigned tasks.	No limitations

Data Category	**Regulated**	**Restricted**	**Public**
Risk Level	High Risk	Medium Risk	Low Risk
	regulated data in their custody.		

Data Category **Risk Level**	**Regulated** High Risk	**Restricted** Medium Risk	**Public** Low Risk
Transmission (Emailing)	Use only secure methods to transmit regulated information.Do not include regulated information in the body of an email or as an attachment. To transmit (email) regulated data to another university email address, use links instead of attachments. Store the regulated information in GW Box and email a link to the file. Regulated data must be encrypted during transmission outside GW network. If there is a business need to email regulated data to non-university recipients, it must be encrypted. To activate encryption of your university email account, submit a GW email Encryption Access Request to GW IT. **Emailing regulated information to or from a personal email address is strictly prohibited.**	Use only secure methods to transmit restricted information. To transmit (email) restricted data to another university email address, use links instead of attachments. Store the restricted information in one of the approved storage systems listed above, and email a link to the file. Restricted data must be encrypted during transmission outside GW network. If there is a business need to email restricted data to non-university recipients, your email account must be encrypted. To activate encryption of your university email account, submit a GW email Encryption Access Request to GW IT. **Emailing restricted information to or from a personal email address is strictly prohibited.**	No limitations
Reproduction	Avoid printing or copying regulated data. The minimum necessary prints / copies may be made only by permission of originator or designates. Working copies (prints) containing regulated data should be secured at all times and permanently destroyed (shredded) when no longer needed. Regulated data should never be printed or copied using a public (non-GW) device. As a general rule, employees are not allowed to take regulated data in physical form off campus (or to make unofficial copies).	Avoid printing or copying restricted data. Only the minimum necessary prints / copies may be made. Working copies (prints) containing restricted data should be secured at all times and permanently destroyed (shredded) when no longer needed. Restricted data should never be printed or copied using a public (non-GW) device. As a general rule, employees are not allowed to make unofficial copies of restricted data.	No limitations
Disposal	Regulated data must be disposed of by using GW IT approved measures, to protect against unauthorized	Restricted data must be disposed by using GW IT approved measures, to protect	No limitations

Data Category	**Regulated**	**Restricted**	**Public**
Risk Level	High Risk	Medium Risk	Low Risk
	access or disclosure. Regulated information must be destroyed in a manner such that the information can neither be reconstructed nor be readable.	against unauthorized access or disclosure.	

▾ Physical Security Best Practices

Physical security is the protection of personnel, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to an institution. When it comes to institutional data physical security controls, faculty and staff should follow the best practices below.

- Restrict physical access to computers when you are away from your office or workspace. For example, locking the door or using security cables or locking devices.
- Secure access to computers and mobile devices by requiring passwords (except for public computers with no Non-Public Information, such as those in the library or in labs). Passwords are integral to security. Follow the GW IT Identity and Access Management Standard for selecting secure UserID passwords and how to reset them. Log out when finished using a GW system.
- Secure access to your computers using a screen saver or built-in lock feature when you are away from your office or work space.
- Maintain possession or control of your mobile devices and apply appropriate safeguards to the extent possible to reduce the risk of theft and unauthorized access.
- In the event that a GW-owned computer or mobile device containing Non-Public Information is lost or stolen, contact GW IT (incident@gwu.edu) immediately.

▸ Applicable University Policies

- Cybersecurity Risk Policy
- Electronic Equipment Recycling
- Laptop Computer and Small Electronics Theft
- Physical Access Policy
- Surplus University Property

Submit a Request

ithelp@gwu.edu
View My Tickets
Reset Password

Classroom Suppor

202-994-7900
Classroom Search

Phone

202-994-4948
24 hours / 7 days a week

Walk-In

Walk-In Support Centers

Knowledge Base

Explore our knowledge base for how-to articles and guides.

IT Help

GW Information Technology

Academic Center
801 22nd Street, NW B101
Washington, DC 20052

Phone: 202-994-GWIT (4948)
ithelp@gwu.edu

Campus Advisories

EO/Nondiscrimination Policy

Website Privacy Notice

Contact GW

Accessibility

Terms of Use

Copyright

Report a Barrier to Accessibility