THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Data Protection Guidance

Information Category Risk Category	Regulated High Risk	Restricted Moderate Risk	Public 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
	Contact your IT Department and/or GW Information Security for further instructions.		
Workstations or Mobile Devices - GW-owned or approved (Desktop, laptop, phone, tablet)	May be accessed, processed, or stored on GW-owned or approved workstations or mobile devices (such devices are configured and managed by the university and must be encrypted). Access must be limited to only Authorized Users on a business "need to know" basis. 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.	May be accessed, processed, or stored on GW owned or approved workstations or mobile devices (such devices are configured and managed by the university and must be encrypted). Access to such information must be limited to only authorized users. The following security controls must be in place: • Password • Remote wiping capability • Registered with the GW IT mobile device management service	No limitations
	Contact your IT Department and/or GW Information Security for further instructions.		
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. 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 • 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
	Contact your IT Department and/or GW Information Security for further instructions.		
Storage	May be used, stored, shared, or processed only on GW hosted or approved servers or services (such as file sharing or collaboration services, cloud- based email services, cloud-based backup and recovery May be stored in the following GW systems: GW Box-GW Documents-Windows File 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.	May be stored on departmental, GW IT-hosted, or approved cloud-based systems May be stored in the following GW systems:-GW G-Drive-GW SharePoint, GW Box and GW Docs. Restricted data in physical form (paper, media) should secured at all times and access should be restricted only to authorized users, with a legitimate business need.	No limitations
	Contact your IT Department and/or GW Information Security for further instructions.		

Information Category Risk Category	Regulated High Risk	Restricted Moderate Risk	Public Low Risk
Emailing	Must be encrypted during transmission outside GW network. It's always preferable to use the strongest cipher available when transmitting Regulated Information, especially when transmitting to a third party. Emailing Regulated Information to and from a personal email address is strictly prohibited.	Must be encrypted during transmission outside GW network. Emailing Restricted Information to and from a personal email address is prohibited.	No limitations
	Contact your IT Department and/or GW Information Security for further instructions.		
Reproduction	The minimum necessary copies may be made only by permission of originator or his/her designates.	The minimum necessary copies may be made only by employees. Contractors and Third parties must sign appropriate nondisclosure agreement or act within the boundaries of the appropriate contract.	No limitations
	Contact Privacy@gwu.edu for further guidance.		
Destruction/ disposal	Must be disposed of by using GW IT approved measures to protect against unauthorized access or disclosure. Regulated information must be destroyed in a manner such that the information can neither be reconstructed nor be readable.	Must be disposed of using GW IT approved measures to protect against unauthorized access or disclosure.	No Restrictions
	Contact GW Information Security for further guidance on destruction / disposal of electronic regulated and restricted data. Contact GW Procurement for shredding services.		