

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Data Protection Guidance

Information Category Risk Category	Regulated High Risk	Restricted Moderate Risk	Public Low Risk
Network	<p>All network traffic must be encrypted in transit using at least TLS v1.1. (TLS v1.2 is strongly encouraged)</p> <p>It's always preferable to use the strongest cipher available when transmitting Regulated Information, especially when transmitting to a third party.</p>	<p>All network traffic must be encrypted in transit using at least TLS v1.1.(TLS v1.2 is strongly encouraged)</p>	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)	<p>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).</p> <p>Access must be limited to only Authorized Users on a business "need to know" basis. The following security controls must be in place:</p> <ul style="list-style-type: none"> • Strong Password • Encryption • Remote wiping capability • Registered and managed by the GW IT mobile device management service. 	<p>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).</p> <p>Access to such information must be limited to only authorized users. The following security controls must be in place:</p> <ul style="list-style-type: none"> • 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)	<p>Regulated or Restricted information may not be downloaded, stored or synchronized on personally-owned workstations or mobile devices.</p> <p>GW Storage systems approved for Regulated Information may be accessed but not installed.</p> <p>Requirements for accessing Regulated Information from personally-owned workstations or mobile devices are:</p> <ul style="list-style-type: none"> • 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 <p>Firmware and driver updates should be installed within a reasonable period</p>		No limitations
Contact your IT Department and/or GW Information Security for further instructions.			
Storage	<p>May be used, stored, shared, or processed only on servers or services (such as file sharing or collaboration services, cloud-based email services, cloud-based backup and recovery services, etc.)</p> <p>May be stored in the following GW systems: GW Box-GW Documents-Windows File</p> <p>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.</p>	<p>May be stored on departmental, GW IT-hosted, or approved cloud-based systems</p> <p>May be stored in the following GW systems: -GW G-Drive-GW SharePoint, GW Box and GW Docs.</p> <p>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.</p>	No limitations
Contact your IT Department and/or GW Information Security for further instructions.			

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

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