PROTECTING INFORMATION

GUIDE TO DATA STORAGE AND CUSTODIAL PRACTICES

Office of Compliance and Privacy | 202-994-3386 | comply@gwu.edu | http://compliance.gwu.edu

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

	Regulated Information	**Restricted Information**	**Public Information**
Examples	Personal health information • Past, present, or future physical or mental health condition • Provision of health care Student academic and financial records • Grades/enrollment details • Financial aid, student bills • Disciplinary action Research data that is protected by statute or regulation. Personally Identifiable data • Social security numbers	• Course information/Class Schedules • Internal directory information • Calendars • Internal GW Email • Payroll/Tax data • HR Data • Salary/Benefits • Performance appraisals • Access codes • Wire Transfers • Payment History • Legal Records/ Contracts/Legal Filings • Financial records and accounts • General Ledger data • Facilities/Physical Plant records • Library records • Accreditation records	• Announcements/Press Releases • Public event information • Public Directories and Maps
Data Storage Security Requirements	Regulated Information must be permanently stored on GW-owned, authoritative systems of record (e.g. Banner, EAS, GW Documentum) or highly secure, restricted access external services (e.g. NetDocuments) that contractually meet GW security requirements. Regulated Information may be temporarily accessed, processed, or stored on GW-owned workstations that are encrypted while in use.	Restricted Information may be accessed, processed, or stored on: • GW-hosted systems or generally available external services (e.g. Google Docs/Drive/Gmail) that contractually meet GW security requirements, • GW-owned workstations, or • Personal systems owned by Authorized Users.	No limitations
Networking Requirements	All network traffic must be encrypted in transit using SSL or equivalent.		No limitations
Computer Workstation and Laptop Requirements for University Owned or Approved Devices	Regulated Information may be accessed, processed, or stored on GW-owned or approved workstations. These devices must be encrypted and access must be limited to only Authorized Users on a need to know basis.	Restricted Information may be accessed, processed, or stored on GW-owned or approved workstations and laptops. Access to such information must be limited to only Authorized Users.	No limitations
Computer Workstation and Laptop Requirements for Personally Owned Devices that are Not Approved	Regulated Information may not be accessed, processed, or stored on personally owned workstations and laptops that are not approved.	Restricted Information may be accessed, processed, or stored on personally owned workstations and laptops. Access to such information must be limited to only Authorized Users.	No limitations
Mobile Device Requirements for University Owned or Approved Devices (e.g. mobile phones, personal digital assistants, tablets)	Regulated Information may be accessed, processed, or stored on GW-owned or approved mobile devices. Such devices must be configured and managed by the university and the following security controls must be in place: • Strong Password • Encryption • Remote wiping capability • Registered and managed by the Division of IT mobile device management service	Restricted Information may be accessed, processed, or stored on GW-owned or approved mobile devices and the following security controls must be in place: • Password • Remote wiping capability • Registered with the Division of IT mobile device management service	No limitations
Mobile Device Requirements for Personally Owned Devices (e.g. mobile phones, personal digital assistants, tablets)	Regulated Information may not be accessed, processed, or stored on personally owned mobile devices unless the device is registered with the Division of IT mobile device management service prior to accessing data. As part of the registration process, the device owner must agree that in the event that the personally owned device is lost, or there is evidence of an actual or suspected breach, their device may be remotely wiped or requested for investigative purposes.	Restricted Information may be accessed, processed, or stored on personally owned mobile devices. The university recommends user training and awareness if personally owned mobile devices are used to access this type of information. Personally owned mobile devices should be enabled with password protection and have the capability to remote wipe. Please contact the IT Support Center for details.	No limitations