PROTECTING INFORMATION: **GUIDE TO GW'S INFORMATION MANAGEMENT POLICIES**

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

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

Managing information is a shared responsibility. Information includes both electronic and physical records such as paper documents and files.

The George Washington University's Information Security Policy and Records Management Policy guide faculty and staff in understanding the responsibilities and consequences of managing university information regardless of format.

For more information, visit **http://compliance.gwu.edu**.

What types of information need to be protected?

Regulated and Restricted data are considered non-public, meaning they are not intended to be shared with the general public and need to be protected. The chart below will help you determine the category of data you may work with in your role at GW. More information about types of data and how to protect it can be found in the Information Security Policy.

INFORMATION SECURITY POLICY

REGULATED INFORMATION IS PROTECTED BY LOCAL, NATIONAL OR INTERNATIONAL STATUTE OR REGULATION MANDATING CERTAIN RESTRICTIONS. EXAMPLES INCLUDE:

- 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*

RESTRICTED INFORMATION MUST BE LIMITED TO APPROPRIATE UNIVERSITY FACULTY, STAFF, STUDENTS OR OTHER AUTHORIZED USERS WITH A VALID BUSINESS NEED. THIS INFORMATION MUST BE PROTECTED FROM UNAUTHORIZED ACCESS, USE OR DISCLOSURE DUE TO UNIVERSITY POLICIES, CONTRACT OR DESIGNATION, OR DUE TO PROPRIETARY OR PRIVACY CONSIDERATIONS. EXAMPLES INCLUDE:

- Course information/class schedules
- Internal directory information
- Calendars
- Internal GW e-mail
- 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
- GWid

PUBLIC INFORMATION HAS NO RESTRICTIONS ON ACCESS, USE OR DISCLOSURE UNDER UNIVERSITY POLICY, OR CONTRACT, OR LOCAL, NATIONAL OR INTERNATIONAL STATUTE OR REGULATION. EXAMPLES INCLUDE:

- Announcements/press releases
- Public event information
- Public directories and maps

How do I know if my GW computer, equipment or network is secure?

- *GW's Division of IT is primarily responsible for securing university-owned systems, equipment and networks. You can help by protecting and securing your equipment and data and by utilizing strong passwords.*

What am I responsible for?

- *Understanding the requirements involved with having custody of certain types of data.*
- *Protecting, using, storing and disposing of data properly.*

What are schools and divisions responsible for?

- *Enforcing behaviors, processes and practices to help protect university data.*

RECORDS MANAGEMENT POLICY

Records management is essential to information management and required by the new Records Management Policy. Schools and divisions are responsible for:

- *Developing procedures and practices to manage records in their custody regardless of format.*
- *Securing non-public records in accordance with the Information Security Policy.*
- *Maintaining any records relevant to any pending or anticipated litigation, claim, audit, agency charge, investigation or enforcement action.*
- *Transferring records of permanent value to University Archives.*
- *Disposing of records following the procedures for the Records Management Policy.*