THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Data Classification Levels

Data custodians are responsible for reviewing and determining the types of non-public information in their custody, based on its sensitivity and confidentiality, by classifying it in accordance with the classification levels described below:

REGULATED

Regulated Data is information that is protected by local, national, or international statute or regulation mandating certain restrictions.

Regulated information constitutes an area of critical concern because of the severe risk to the university, its affiliates and to individuals, should information be inappropriately accessed, altered, disclosed or destroyed.

Regulated information requires strict control, very limited access and disclosure, which may be subject to legal restrictions. Access to regulated data must be limited to authorized university employees (staff and faculty) with a valid business need. Where access to regulated data has been authorized, use of such data shall be limited to the purpose required to perform university business. Authorized users must respect the confidentiality and privacy of individuals whose regulated information they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

Examples of regulated data include:

- student academic and financial records, regulated by FERPA
- Protected health information (PHI), regulated by HIPAA
- other forms of regulated information include social security numbers, export controlled data and information (excluding technology or software that arises during, or results from, fundamental research under Section 734.8 of the EAR), and credit card information.

RESTRICTED

Restricted Data is information that is not generally available to the public, but deemed confidential due to university policies, contracts, regulations or due to proprietary considerations.

Access to restricted data 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. If disclosed, altered or destroyed, restricted data could cause a moderate adverse impact to the individual, university or its affiliates.

Examples of restricted data include:

- payroll and tax information, performance appraisals
- legal records and contracts;
- general ledger data, Facilities records
- internal directory information

PUBLIC

Public Data is information that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage.

Security controls are required to protect public data, against unauthorized modification or destruction. If altered or destroyed, public data would cause little or no adverse impact to the university, its affiliates, or the individual.

Example of public data include:

- announcements and press releases
- public event information
- public directories and maps