DCL In a Nutshell

Data classification levels are extremely complex – and extremely important to follow. The information here gives a very brief overview of how different types of data are labelled and how they should be handled.

Highly Restrictive

DCL4

Treatment:

Do not disseminate.

Mishandling of DCL 4 Data will have very serious repercussions for the University.

- Follow governing statutes with specific provisions for protection.
- Data at rest must be encrypted when technically feasible.
- All logs must be forwarded to the university-provided centralized logging service.

Examples:

- Biometric Data
- E-Commerce
- Export Controlled (can't leave the U.S.)
- National Security
- HIPAA-Protected Health Info
- SSNs

Restrictive

DCL3

Treatment:

Disseminate following regulatory and legal requirements.

- Databases must be segregated from front-end systems.
- No inbound Internet access except through an approved exception.
- Servers must be housed in a centrally managed data center.

Examples:

- FERPA Data
- Personally Identifiable Information
- Birthdate/Address/ID Number
- Proprietary or Protected Research

Sensitive

DCL2

Treatment:

Disseminate only to those with a need to know, by someone with authorization.

- End-user access must be authenticated.
- Access reviewed quarterly for appropriateness.
- Access revoked as soon as employee leaves department.

Examples:

- Budget
- Salaries
- Personal Phone Numbers
- Departmental Policies/Procedures
- Internal Memos
- Unpublished Research

Public

DCL1

Treatment:

Disseminate freely.

- Host-based firewalls required.
- Antivirus required.

Examples:

- Ads
- Product and Service Info
- Directory Listings
- Presentations
- Published Research
- Job Postings
- Press Releases

022415