## 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.

<table>
<thead>
<tr>
<th>DCL Level</th>
<th>Treatment</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Highly Restrictive</strong></td>
<td>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.</td>
<td>Biometric Data, E-Commerce, Export Controlled (can’t leave the U.S.), National Security, HIPPA-Protected Health Info, and SSNs</td>
</tr>
<tr>
<td><strong>Restrictive</strong></td>
<td>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.</td>
<td>FERPA Data, Personally Identifiable Information, Birthdate/Address/ID Number, Proprietary or Protected Research</td>
</tr>
<tr>
<td><strong>Sensitive</strong></td>
<td>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.</td>
<td>Budget, Salaries, Personal Phone Numbers, Internal Memos, Unpublished Research</td>
</tr>
<tr>
<td><strong>Public</strong></td>
<td>Disseminate freely. • Host-based firewalls required. • Antivirus required.</td>
<td>Ads, Product and Service Info, Directory Listings, Presentations, Published Research, Job Postings, Press Releases</td>
</tr>
</tbody>
</table>