<table>
<thead>
<tr>
<th>Mission-Critical (Restricted)</th>
<th>Restricted</th>
<th>Secure</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>System-wide obligation to protect the data and resurrect full operation as first priority.</td>
<td>Protection of this type of data is required by law, UC or UCB policy, or data proprietor (HIPAA, FERPA, EPCA, sb1386, etc.).</td>
<td>Individual organization or research group’s obligation.</td>
<td>Public accessible information.</td>
</tr>
</tbody>
</table>

**Examples:**
- Student information (SIS, admission)
- Personnel (HRMS, payroll).
- Institutional financial databases (BFS)
- Contracts (ORU, federal and state grants).
- Networking services.
- Emergency response.

**Examples:**
- Personal identifiable data, such as passwords, digital certificates.
- Physical plant details (emergency preparedness and incident response plans).
- NDA (or incomplete research results).
- Financial or budgetary projections and transactions.
- Student information (grades).
- Donor or prospect information.
- Credit cards.
- Other confidential information (client-attorney, ombuds, health records).
- Patent information (prior to approval).

**Examples:**
- Personal data not in previous two categories (contact, location, etc.).
- Email (except those containing data in the previous two categories).
- Email addresses and mailing lists.
- Privileged forms or access rights (accessible via web).
- Campus maps, phone directories, office locations.

**Examples:**
- Web content (excluding those with data in the previous three categories).
- Research simulations or test data.
- FAQ.
- Searchable, indexed data.
- Developmental servers.

**Impact:**
- Financial or operational loss on an institutional level.
- Loss of federal or state grants/funding.

**Impact:**
- Financial loss on a personal or group level.
- Personal identity theft.
- Institutional security.
- Privacy.

**Impact:**
- Personal or group physical security.
- Personal privacy.
- Misuse or abuse.
- Loss of productivity.

**Impact:**
- Minimal loss of productivity.
- Inconvenience.

**Required Actions:**
- Submit business continuity and security plan (be reviewed periodically and audited by campus).
- Requires dedicated professional system management, preferably 24x7.
- TPOC must go thru background checks.
- System activities will be monitored and reviewed.
- Access needs to be minimal, controlled, and monitored.
- Physical security must be maintained.
- Transmission of this data over unencrypted media is not allowed (such as wireless).

**Required Actions:**
- Require a security plan.
- Systems hosting this data require professional system management.
- TPOC subject to background checks.
- Disaster recovery plan is recommended.
- Access be restricted, authenticated, and monitored.
- Authorization to modify data should be logged and reviewed.
- Systems storing partial or full restricted data should have the same security measures.
- Data retention and salvage process should satisfy UCB requirements.
- Transmission of this data over unencrypted media is not allowed (such as wireless).

**Required Actions:**
- Systems hosting these data should be professionally managed.
- Systems should satisfy campus “minimum security requirement” and other requirements as necessary.
- User must conform with campus policies in order to use campus accounts.
- Authorization to modify the data should be restricted.

**Required Actions:**
- Open access.
- Satisfy campus “minimum security requirement”.
- Participate in all required user level trainings.