### Classification

<table>
<thead>
<tr>
<th>Low Risk (Green)</th>
<th>Moderate Risk (Amber)</th>
<th>High Risk (Red)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data is classified as Low Risk (&quot;green&quot;) if the loss of confidentiality, integrity, or availability of the data would have minimal strategic, compliance, operational, financial, or reputational risk to the University.</td>
<td>Data is classified as Moderate Risk (&quot;amber&quot;) if the loss of confidentiality, integrity, or availability of the data would have moderate strategic, compliance, operational, financial, or reputational risk to the University.</td>
<td>Data is classified as High Risk (&quot;red&quot; - the most sensitive/critical classification) if the loss of confidentiality, integrity, or availability of the data would have high strategic, compliance, operational, financial, or reputational risk to the University.</td>
</tr>
</tbody>
</table>

### Data Types:

- **Non-sensitive Course or Program Information**
- **Non-sensitive Research Information**
- **Student Records (directory information)**
- **Disaster recovery/business continuity plans**
- **Electrical, Steam, Chiller Utility data**
- **Human Resource Search Files**
- **Library Transactional Data**
- **Personnel Files**
- **Student Records (non-directory)**
- **University Financial Records**
- **Disaster recovery/business continuity plans**
- **Architectural diagrams for the physical spaces where critical systems or functions exist (ex. Animal Labs, Datacenters, Mechanical Rooms)**
- **Attorney-Client Privileged and/or Attorney Work-Product Information**
- **Common Composite High Risk Data**
- **Controlled Unclassified Information (CUI) – Research**
- **Customer Card Data (PCI DSS)**
- **Disability-Related Medical Information**
- **Identifiable Human Subject Data - Research**
- **Information System Configuration**
- **Internal Audit Working Papers**
- **Items Covered by Contractual Non-Disclosure or Data Use Agreement**
- **Law Enforcement Information (LEI)**
- **Personally Identifiable Information (PII) (SSNs, date of birth, DL numbers)**
- **Protected Health Information (PHI)**
- **Private Personal Information (PPI)**
- **Sensitive Alumni, Donor or Constituent Information**
- **Sensitive Intellectual Property – Research**
- **Sensitive Security Data**
- **Student Financial Aid Data (GLBA)**
- **Workers Compensation**

### Know the policies:

The full policy and additional resources are at [https://infosec.uoregon.edu/policies-procedures-and-standards](https://infosec.uoregon.edu/policies-procedures-and-standards)

### Seek assistance:

If you have questions or concerns about the policy, or if you know of items that are out of compliance, please contact your manager or the ISO Office.

### Use good judgment:

The lists above are only examples, not an exhaustive list.

Publication Date: 03/26/2020 Version 1
**Information Security Quick Reference**

General Safeguards for Moderate Risk and High Risk data:
- Share only with those authorized to have access
- Use caution when discussing in public places
- Secure paper-based information in locked desk/office/cabinet when not in use
- Report possible or actual loss immediately to your supervisor or the Information Security Office

### HANDLING

<table>
<thead>
<tr>
<th>Activity by Data Classification</th>
<th>Moderate Risk (Amber)</th>
<th>High Risk (Red)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printing</td>
<td>Do not leave unattended on copiers/printers</td>
<td>Only print if you absolutely need to. Do not leave unattended on copiers/printers</td>
</tr>
<tr>
<td>Mailing paper-based info</td>
<td>Put in a sealed envelope/box and send via interoffice or USPS mail.</td>
<td>Put in a sealed envelope/box and send via FedEx/UPS/USPS mail with tracking/delivery confirmation where feasible.</td>
</tr>
<tr>
<td>Storing electronic files on work or personal computer (including portable devices)</td>
<td>The University would prefer this work be done on a University issued computer. If a personal computer must be used, it should adhere to UO personal device guidance, including device password, anti-virus, up-to-date patches, and encryption.</td>
<td>Never put red data on a personal computer. Computer must meet UO Minimum Information Security Control Standard, including device password, anti-virus, up-to-date patches, encryption, and system management.</td>
</tr>
<tr>
<td>Storing files on external portable storage media</td>
<td>Physically protect the media</td>
<td>USB stick, CD/DVD, back-up tape, etc. must be encrypted and password protected.</td>
</tr>
<tr>
<td>Sharing files with authorized individuals</td>
<td>Use approved collaboration tools and share with specific authorized individuals, not anonymous or guest links.</td>
<td>Use approved collaboration tools and share with specific authorized individuals, not anonymous or guest links.</td>
</tr>
<tr>
<td>Sending data/files to authorized individuals</td>
<td>Use email and send only to those authorized to view it.</td>
<td>Encrypt when transmitting data both internally and externally: Use a UO-supported Secure File Transfer method (e.g. OneDrive, SFTP). On website forms, use HTTPS.</td>
</tr>
<tr>
<td>Engaging vendors to store/process data</td>
<td>Ensure vendor/hosting agreement includes UO’s data security addendum.</td>
<td>Engage the Information Security Office for a security review and include UO’s data security addendum in the vendor/hosting agreement.</td>
</tr>
<tr>
<td>Deleting electronic files</td>
<td>Use the standard Delete/&quot;X&quot; commands and empty the trash bin</td>
<td>Use a secure delete or overwrite data</td>
</tr>
</tbody>
</table>

**How to dispose/recycle paper**

- **Low Risk (Green)** Data only for single-stream recycling
- **Moderate Risk (Amber) and High Risk (Red)** Data to be shredded and recycled

**How to dispose of devices and/or prepare them for recycling or upgrade**

- **Shred CD/DVD at provided shredders or contact local IT Support**
- **Contact local IT Support for pick-up or drop-off:** they will remove data and recycling

**Publication Date: 03/26/2020 Version 1**