# Data Classification levels

**Regulated Data** is data that if disclosed, altered or destroyed, could cause a significant adverse impact to the individual, university or its affiliates. Regulated data is protected by local, national, or international statute or regulation mandating certain restrictions. **Access**: Limited to a legitimate business need. **Safeguarding**: This information must be protected from unauthorized access, use or disclosure due to university policies, contract, or designation, or due to proprietary or privacy considerations. **Examples**: 
- Student academic and financial records
- E.g. Grades/enrollment details, financial aid student bills, Disciplinary actions
- Personal Health Information
- E.g. Past, present, or future physical or mental health condition, Provision of health care
- Personal Identifiable Information (e.g. SSN)
- Research Data protected by statute or regulation

**Restricted Data** is data that if disclosed, altered or destroyed, could cause a moderate adverse impact to the individual, university or its affiliates. **Access**: Limited to a legitimate business need. **Safeguarding**: This information must be protected from unauthorized access, use or disclosure due to university policies, contract, or designation, or due to proprietary or privacy considerations. **Examples**: 
- Course information and schedules
- Payroll and tax data, HR data, payment history and information on Access codes, legal records and contracts; general ledger data, Facilities
- Restricted records

**Public Data** is data that if disclosed, altered or destroyed, would cause little or no adverse impact to the university, its affiliates, or the individual. **Access**: Open **Safeguarding**: Little or no controls are required to protect the confidentiality of Public data, yet, some level of control is required to prevent unauthorized modification or destruction of it. **Examples**: 
- Announcements / press releases
- Public event information
- Public directories and maps;
### Practical Guide for Classifying University Data

- Is data/information protected by local, national or international statute or regulation mandating certain restrictions? **YES**
  - **REGULATED**

- Is it Personal Data (information)? **NO**
- Does data allow a person to be identified? **NO**
- Will personal data be collected in and/or transmitted to/from another country? **NO**

- Does data contain information that is limited to appropriate university personnel with a valid business need? **NO**

- Is data/information considered acceptable for public release? **YES**
  - **PUBLIC**

### Data Protection Guidance

<table>
<thead>
<tr>
<th>Information Category</th>
<th>Regulated</th>
<th>Restricted</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Category</strong></td>
<td>High Risk</td>
<td>Moderate Risk</td>
<td>Low Risk</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>All network traffic must be encrypted in transit using at least TLS v1.1. (TLS v1.2 is strongly encouraged). It's always preferable to use the strongest cipher available when transmitting Regulated Information, especially when transmitting to a third party.</td>
<td>All network traffic must be encrypted in transit using at least TLS v1.1. (TLS v1.2 is strongly encouraged).</td>
<td>No limitations</td>
</tr>
</tbody>
</table>
| **Workstations or Mobile Devices - GW-owned or approved** (Desktop, laptop, phone, tablet) | May be accessed, processed, or stored on GW-owned or approved workstations or mobile devices (such devices are configured and managed by the university and must be encrypted). Access must be limited to only those authorized users on a business “need to know” basis. The following security controls must be in place:  
  - Strong Password  
  - Encryption  
  - Remote wiping capability  
  - Registered and managed by the GW IT mobile device management service. | May be accessed, processed, or stored on GW-owned or approved workstations or mobile devices (such devices are configured and managed by the university and must be encrypted). Access to such information must be limited to only authorized users. The following security controls must be in place:  
  - Password  
  - Remote wiping capability  
  - Registered with the GW IT mobile device management service. | No limitations |
| **Personally-Owned Devices** (Desktop, laptop, phone, tablet) | Regulated or Restricted information may not be downloaded, stored or synchronized on personally-owned workstations or mobile devices. GW Storage systems approved for Regulated Information may be accessed but not installed. Requirements for accessing Regulated Information from personally-owned workstations or mobile devices are:  
  - Full Disk Encryption (FDE)  
  - Use of VPN  
  - Must be password protected  
  - Anti-Virus / Anti-Spyware software must be active and maintained up to date  
  - Updates for all installed software should be installed within a reasonable period. Firmware and driver updates should be installed within a reasonable period. | May be used, stored, shared, or processed only on servers or services (such as file sharing or collaboration services, cloud-based email services, cloud-based backup and recovery services, etc.)  
  - May be stored in the following GW systems: Box, GW SharePoint, Box and GW Docs.  
  - Restricted data in physical form (paper, media) should be locked at all times and access should be restricted only to authorized users, with a legitimate business need. | No limitations |

Contact your IT Department and/or GW Information Security for further instructions.