**Objective:** To determine if the department/unit has procedures for backing up and recovering institutional information which are reviewed/updated periodically. Additionally, to determine if employees are performing approved local backups or storing on ITS provided storage infrastructure and adequate protection/storage exists for backups.

**Risk Level/Potential Impact:** High; Results in loss of data which could greatly reduce the ability of the department/unit to maintain daily operations if information system back-ups are not performed on a regular basis, stored in a secure location and if recovery procedures are not in place and tested. Additionally, may result in financial loss as well as subject the institution to negative publicity.

**Criteria:** Institutional policies and procedures; Best business practices.

**Frequently Observed Weaknesses/Deficiencies:**
- Lack of back up procedures.
- Failure to back up information on a regular basis.
- Failure to use approved secure share drives to store data.
- Storing backups in the same office and/or building as the computer housing the information.
- Loss of unencrypted backup media.
- Failure to have recovery procedures/plans.
- Undocumented recovery procedures/plans.
- Failure to perform recovery testing.
- Failure to have a central area for software media and a backup copy, with vendor contact and license keys, stored off-site.

**Helpful Tools:**
- Information Technology Support and Services – [https://paws.gru.edu/pub/its/](https://paws.gru.edu/pub/its/)
- Policies – [http://policy.gru.edu/](http://policy.gru.edu/)

---

**Helpful Tools Continued:**
- Data Management and Classification
- Enterprise Data Storage and Backup Policy
- IT Configuration Standards Policy
- Mobile Device Policy

**GRU Contact Office and Information Resource(s):** Division of Information Technology Services (706) 721-4000.

**Best Business Practices:**
1. Management should appoint a data steward and manager for overseeing information systems processes to include back up procedures.
2. Require employees to store institutional data on an Information Technology Services (ITS) approved data storage location (e.g. a secure share or home directory).
   - Institutional Data is any data created/collected in pursuit of achieving the institutional mission.
3. Physically secure removable and/or mobile storage media containing restricted and/or regulated data.
4. Ensure human research data is stored ONLY on the R-drive.
5. Ensure procedures exist for the backup of information on mobile assets such as laptops, USB and flash drives to include the use of encryption for restricted and/or regulated data.
6. Backups should be stored in a secure location and should not be stored in the same office and/or building as the computer housing the information.
7. Management of the department/unit should work with ITS to coordinate efforts to ensure disaster recovery procedures are developed and adequately documented. The resource owner for the department/unit must identify critical resources to be protected.
8. Perform recovery testing on a periodic basis.
9. Document recovery testing and analyze results. Make improvements to recovery procedures as needed.
10. Ensure recovery plans are revisited periodically for necessary revisions and updates.
11. Keep a backup of important software, license keys, and vendor contact information off-site.
## Self-Assessment of Internal Controls for Data Back-Up

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a procedure in place and reviewed/updated periodically for departmental backups of institutional data?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is institutional data stored on an ITS supported network server?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If data are backed up or stored on mobile media (i.e. USB, flash, CD-ROM, laptop, tablet, etc.), is the restricted and/or regulated data encrypted and secured?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is backup media stored in a different location than source data?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there an inventory for institutional data not stored on ITS-provided storage infrastructure?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the department identified all required IT software and/or equipment (i.e. printers, scanners, laptops, microscopes) that are connected to computing devices?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do employees have adequate training and/or knowledge of data backup and recovery?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>