**Objective:** To determine whether the department/unit practices record and electronic data retention that is compliant with institutional, BOR, federal and state law retention policies and procedures.

**Risk Level/Potential Impact:** High; Results in noncompliance with institutional and/or BOR policies, placing the institution in potential violation of federal and state laws exposing the institution to negative publicity.

**Criteria:** Institutional and BOR retention guidelines; Federal and state laws.

**Frequently Observed Weaknesses/Deficiencies:**
- Failure to have records retention practices.
- Failure to periodically communicate information on records retention.
- Maintaining records beyond required retention period.
- Failure to secure records.
- Failure to obtain a certificate of destruction documenting what and when records were destroyed.
- Not utilizing Augusta Data Storage’s records retention and document destruction services.
- Failure to archive electronic data.
- Failure to back up electronic data.

**Helpful Tools:**
- GRU Administrative Policies and Procedures Index - [http://policy.gru.edu/](http://policy.gru.edu/)
- GRU Records Retention Policies - [http://policy.gru.edu/](http://policy.gru.edu/)

**Helpful Tools Continued:**
- BOR Records Retention Policies - [http://www.usg.edu/records_management/](http://www.usg.edu/records_management/)
- Policy 8.2.2 Extra Duty Compensation – [http://policy.gru.edu/](http://policy.gru.edu/)

**GRU Contact Office and Information Resource(s):** GRU’s Office of Legal Affairs (706) 721-4018, Office of Institutional Audit and Compliance (706) 721-2661.

**Best Business Practices:**
1. Maintain all required departmental records for the appropriate retention period. Examples: bi-weekly timesheets-4 years; Travel Expense Statements-for the respective fiscal year only.
2. Develop internal record retention guidelines/procedures as necessary and ensure communication of these guidelines, as well as GRU’s guidelines to all employees. Additionally, inform users that the information stored electronically (or via computer), including email, may be subject to disclosure under open record laws.
3. Develop and implement storing and purging/destruction policies and procedures. Augusta Data storage should be utilized as needed.

(Notes: Employees are required to manage and destroy confidential records appropriately to protect the privacy of students, patients, individuals, and the institution.)

**Case Scenario:** An office coordinator for a department maintains several years of student files within an office in boxes. These files contain student grades, patient tracking sheets and procedure logs, exam grades, etc. The coordinator also has patient files dating 15 years documenting medical services provided at local community events in this office. The office remains locked; however, the information is not safeguarded within the office and several employees have keys, including master keys. The coordinator shreds records as time permits, but is unsure of how long to maintain certain records. Additionally, when the department administrator is initially asked where and what patient and/or student records may exist in the department, the department administrator is unsure. What concerns and risks are associated with the records in this office?

**Case Scenario Answer:** This scenario contains several concerns related to record retention, record security/safeguarding, and legal liability. The above patient and student information should be secured under lock and key in the coordinator’s office, because access to student and patient records should be restricted to only those with a work-related need. Additionally, the coordinator has no idea of how long to maintain certain records and when to dispose of them because the department does not have internal record retention procedures and has not communicated information to employees on GRU’s records retention guidelines. In this case, these patient records are only required to be maintained ten years from the last date of service and maintaining them longer creates unwarranted safeguarding risks and does not promote efficient and effective use of office space. The department has also not taken steps to identify if and where student and/or patient information exists in the department to ensure that proper protection and retention are established.
**Best Business Practices Continued:**

4. Avoid keeping unnecessary records. *(Note: This could increase GRU’s liability for unauthorized access as well as decrease available storage space.)*

5. Ensure security of all records by limiting access to those who have a job-related need-to-know.

6. Ensure all work-related electronic data is archived and backed up.
## Self-Assessment of Internal Controls for Records Retention

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are employees familiar with institutional, BOR, federal and state policies and procedures regarding records retention?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does management periodically communicate practices regarding records retention including electronic data to employees?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the department developed and implemented policies and procedures for the storing and purging/destruction of records?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the department avoid maintaining unnecessary records so as to maximize efficient use of space?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all records (student, employee, patient) appropriately secured to avoid unauthorized access?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do employees ensure all work-related electronic data is archived and/or backed up?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the department utilize the services offered by Augusta Data Storage?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are records retained for the appropriate time period as prescribed by institutional and BOR policies? Records Management – <a href="http://www.usg.edu/records_management/">http://www.usg.edu/records_management/</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>