Objective: To determine whether the department/unit protects the privacy of student education information.

Risk Level/Potential Impact: Medium to High; Results in negative impact to the student and possibly subject the institution to legal liability, negative publicity, and the loss of Federal funding if private student data is disseminated inappropriately.

Criteria: Federal law; Institutional and BOR policies and procedures; Best business practices.

FERPA - the Family Educational Rights and Privacy Act (1974) is a federal law that protects the confidentiality of student records. Students have specific protected rights regarding the release of educational records and FERPA requires that institutions adhere strictly to these guidelines. Just about any record that contains personally identifiable information that is directly related to the student is considered an educational record under FERPA. There are two types of educational records under FERPA: directory (can be disclosed without written consent of the student) and protected (cannot be disclosed to anyone, including parents, without the prior written authorization of the student).

Frequently Observed Weaknesses/Deficiencies:
- Failure to properly secure student records.
- Releasing student information without proper written authorization.
- Accessing student educational information without a legitimate need related to completing job responsibilities.
- Leaving a stack of graded tests for students to pick up and sort through.
- Discussing student information with anyone (including parents) other than the student or a school official with a work-related need to know without written consent from the student.
- Posting grades.

Helpful Tools:
- FERPA – http://gru.edu/registrar/privacy.php
- Data Management and Classification Policy – http://gru.policytech.com/
- Web Based training for Workforce – train.gru.edu

GRU Contact Office and Information Resource(s): Office of the Registrar (706) 721-1430; GRU’s Compliance and Enterprise Risk Management (706) 721-0900; GRU’s Compliance Hotline (800) 576-6623.

Best Business Practices:
1. Ensure workforce involved with student education information, as well as all students, are aware of FERPA requirements. FERPA requires that GRU annually notify students of their educational privacy rights.
2. Ensure workforce with access to and work-related responsibilities for student education information have signed GRU’s Confidentiality Statement.
3. Ensure all requests for FERPA-protected records are routed through the Office of the Registrar.
4. Examples of FERPA-protected student information include: social security number, student identification number, race, ethnicity, nationality, gender, transcripts, and grade reports.
5. Directory information is limited to the following: name, address, telephone number, photograph, email address, dates of attendance, degrees awarded, enrollment status, and major field of study. This information may be disclosed without student consent; however, a student may restrict the disclosure of this information by annually notifying the registrar in writing by the last day of fall registration (or the initial registration if other than fall) that he/she does not want the information released.
6. Consider information in student records confidential and do not disclose/release, except as allowed by law and GRU policy. GRU may not disclose non-directory student information without a GRU work-related need or prior-written authorization by the student. Students must submit a signed release to the Office of the Registrar authorizing a disclosure and the Office of the Registrar will direct the student and/or department personnel appropriately.
Best Business Practices Continued:

7. When in doubt about releasing student records, contact the Office for Compliance and Risk Management’s enterprise privacy officer.
8. Ensure records are properly safeguarded to avoid unauthorized access and improper disclosure.
9. Ensure safeguarding measures are taken to reasonably protect student information that is copied and/or received/sent via fax or email.
10. Utilize sealed confidential envelopes when protected student information is transferred between authorized individuals.
11. Avoid emailing grades. Grades may be directed to the wrong individual.
12. Avoid using the entire social security number of a student to publicly post grades.
13. Never leave graded tests in a stack for students to pick up by sorting through the papers of all students.

Case Scenario: Mrs. Smith, the mother of Lisa Smith who is a student at GRU, telephones Dr. Taylor. Dr. Taylor is her daughter Lisa’s professor. Mrs. Smith explains that she has been very concerned about Lisa’s grades and asks Dr. Taylor to tell her how her daughter is performing in school. Dr. Taylor does not have written consent from the student to release this information; however because the mother seems so concerned, he feels certain it is ok. Dr. Taylor reviews Lisa’s records and tells Mrs. Smith that Lisa has all A’s in her classes and that there is no need to worry. Did Dr. Taylor violate FERPA by providing this information?

Case Scenario Answer: Yes, the student did not authorize release of her educational information. This violates FERPA and as well as GRU’s policies.

Case Scenario: Professor Frank receives a call from the local police department. Officer James explains that he is in the middle of an investigation and is wondering if Lyle Maddox was in class the week before on Friday, July 10th. Professor Frank checks his attendance records for class that day and tells Officer James, yes, Lyle was in class on that Friday. Is this a violation of FERPA?

Case Scenario Answer: Yes, the officer should have been directed to the Office of the Registrar so that appropriate procedures could be followed prior to release of such information.
### Self-Assessment of Internal Controls for Family Educational Rights and Privacy Act (FERPA)

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does workforce of the unit only disclose protected student information as directed by the Office of Registrar when an authorized release has been submitted?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have all workforce (faculty, staff, temporaries, contractual employees and students) of the department/unit signed GRU’s Confidentiality Statement?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is workforce involved with protected student information familiar with FERPA?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the department/unit periodically communicate information regarding FERPA to all students and employees?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is workforce aware of what is directory and non-directory information?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are records properly safeguarded to avoid unauthorized access and improper release?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are safeguarding measures taken to reasonably protect student information that is being copied and/or received and sent via fax?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are sealed confidential envelopes utilized when student information is being transferred between authorized individuals?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the practice of emailing grades avoided?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>