Regent University Information Security Training Policy

Introduction

Regent University places significant importance on the security of student educational records, student and employee financial information and personally identifiable information (PII). To that end, an Information Security Awareness Training program is in place to ensure that all Regent employees are well versed in the legal requirements, University policies, procedures, tools and technical controls aimed at securing this information.

Audience

The Information Security Training Program applies to all Faculty, Staff and Student Workers at Regent University. Additional training and compliance requirements apply to employees with access to PII, educational records or financial information. A designated Point of Contact (POC) is appointed in each department handling sensitive information (such as the Student Financial Aid Office), designated with coordinating compliance with this policy. All employees are required to reaffirm awareness and compliance with these policies on an annual basis.

Awareness

The Information Security Awareness Training program includes reminders of the University policies and legal requirements to keep student and employee information secure and confidential. These include:

- Regent University Information Security Policy
- Regent University Information Security Training Policy
- Regent University Information Systems Acceptable Use Policy
- Regent University Electronic Mail Policy
- Regent University Network Connectivity Policy
- Regent University Password Policy
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act (FERPA)

Employees are required to acknowledge understanding of these policies and legal requirements.

Storage of Sensitive Information

Training regarding the safe storage of student educational records and student and employee financial records and PII includes the following:

- Locking rooms and storage containers where records are kept.
- Keycard and physical access controls to data centers where records are stored.
- Verifying identity and rights to access information when a record request is made.
- Use of encryption and proper access controls on digital records.

- Securing any devices used to access sensitive information, including personal devices, and requiring drive encryption on employee laptops.
- Use of endpoint anti-virus and other digital security controls to prevent data breaches, and procedures to report suspected intrusions to the IT Security department.
- Strong password requirements, prohibiting the use of shared passwords and encouraging the use of Multi-Factor Access (MFA) controls where appropriate.

Transmitting Sensitive Information

Training regarding the secure transmission of student educational records and student and employee financial records and PII includes the following:

- Prohibiting the use of insecure methods of transmitting physical records (such as unsecured fax lines).
- Prohibiting the use of insecure methods of transmitting digital records (such as unencrypted email, insecure file transfer or non-vetted 3rd party file storage vendors).
- Requiring the use of encryption and password protection where applicable at the file and network level for transmitting sensitive information.
- Recognizing and avoiding scam or phishing attempts to access University systems, networks or information directly.

Auditing Access to Sensitive Information

Training regarding audits to ensure proper access to and safe disposal of sensitive information includes the following:

- Department inventories of computer assets storing sensitive records and personnel with access to those records.
- Procedures to notify the Information Technology department when employee roles change, or employment is terminated, to ensure proper access is adjusted or removed when required.
- Key security requirements to verify with partners and 3rd party vendors (such as Software as a Service, or SaaS, vendors) with potential access to student or employee sensitive information.
- Procedures for secure disposal of both physical and digital sensitive records when they are no longer needed.
- Procedures for notifying IT in the event of a suspected or potential data breach.
- Procedures for notification of owners, stakeholders, law enforcement and/or credit bureaus in the event of a data breach.

Named Points of Contact

Jonathan Harrell – Assistant Vice President of Information Technology
Steve Baskerville – Director of Network Engineering
Ben Golub – Information Security Training Program Coordinator

Rachel Moser – Director of Student Financial Aid

Steven Bruce – VP for Business Administration

Martha Smith – VP for HR and Administration

Louis Isakoff – SVP and General Council

References

https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html