Policy 5.11
Critical Financial Reporting Systems Security Policy

Responsible Official: Enterprise CIO and Sr. Vice Provost for Library Services and Digital Scholarship
Administering Division/Department: LITS: Library & IT Services
Effective Date: February 04, 2009
Last Revision: July 24, 2017

Policy Sections:
I. Overview
II. Applicability
III. Policy Details
IV. Definitions
V. Related Links
VI. Contact Information
VII. Revision History

Overview

This policy documents information security controls that are intended to ensure the integrity of information systems and data which are critical for accurate annually audited financial reporting. New systems added which meet this criteria are expected to comply within 60 days of implementation.

Applicability

This policy applies to all information systems which have been deemed critical for accurate annually audited financial reporting (Critical Financial Reporting Systems) by the EVP, Business and Administration or designee. At the time of this revision, the following information systems have been identified as Critical Financial Reporting Systems:

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Business Owner(s)</th>
<th>System Owner(s)</th>
<th>Technical Owner(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAR - Gift/Pledge/Constituent System</td>
<td>Ben Tompkins</td>
<td>Josh Greenbaum</td>
<td>Josh Greenbaum</td>
</tr>
<tr>
<td>Bank of America Treasury Mgmt System*</td>
<td>Carol Kissal</td>
<td>John Hallay</td>
<td>Tom Vincent - Integrations</td>
</tr>
<tr>
<td>Bank of New York Mellon Treasury System</td>
<td>Carol Kissal</td>
<td>John Hallay</td>
<td>Tom Vincent - Integrations</td>
</tr>
<tr>
<td>Blackline**</td>
<td>Carol Kissal</td>
<td>Alison Berg</td>
<td>Tom Vincent - Integrations</td>
</tr>
<tr>
<td>Code Red</td>
<td>Chief Investment Officer</td>
<td>Kristi L. Monsour</td>
<td>Francie Ferdinand/Deapiah Harris/Cede Red</td>
</tr>
<tr>
<td>Core - Cashflow System**</td>
<td>Carol Kissal</td>
<td>Michael Jacubenta</td>
<td>Dewayne Harris/Core</td>
</tr>
<tr>
<td>Emory Business Intelligence</td>
<td>Carol Kissal</td>
<td>Belva White</td>
<td>Dana Hargis</td>
</tr>
<tr>
<td>EmoryCard</td>
<td>Carol Kissal</td>
<td>Michael Jacubenta</td>
<td>Shane Grizzle and the Director of EmoryCard</td>
</tr>
<tr>
<td>Fundriver Endowment Software</td>
<td>Carol Kissal</td>
<td>Allison Berg</td>
<td>Tom Vincent - Integrations</td>
</tr>
<tr>
<td>GE Centricity Business - Patient Billing for Emory Univ**</td>
<td>Jimmy Hatcher</td>
<td>Melane Broun</td>
<td>Rhoda Sturz</td>
</tr>
<tr>
<td>Health Quest - Patient Billing for EHC</td>
<td>Jimmy Hatcher</td>
<td>Jim Perry</td>
<td>Rhoda Sturz</td>
</tr>
<tr>
<td>P enrichment Trustee Network**</td>
<td>Carol Kissal</td>
<td>Loette Gossby</td>
<td>Tom Vincent - Integrations</td>
</tr>
<tr>
<td>Revenue Timkeeping System</td>
<td>Carol Kissal/Jimmy Hatcher</td>
<td>John Mitchell/Marlon Ogunley</td>
<td>Karen Henderson/Jenn Meaux</td>
</tr>
<tr>
<td>Prospective Financial Aid</td>
<td>Assistant MD</td>
<td>Beth Bross/Udseth Leach</td>
<td>Dean Schuh</td>
</tr>
<tr>
<td>Prospective Financial Aid</td>
<td>Carol Kissal/Emary Mitchell</td>
<td>Steve Mandel/Mark Aymard</td>
<td>Tom Vincent</td>
</tr>
<tr>
<td>Prospective Human Resources</td>
<td>Assistant MD/Carol Kissal</td>
<td>Peter Boulgranize/Deapiah Harris</td>
<td>Karen Hargis</td>
</tr>
<tr>
<td>Prospective Payroll</td>
<td>Carol Kissal/Emary Mitchell</td>
<td>John Mitchell/Marlon Ogunley</td>
<td>Karen Henderson</td>
</tr>
<tr>
<td>Prospective Financial Aid</td>
<td>Assistant MD/Carol Kissal</td>
<td>Steve Mandel/Mark Aymard</td>
<td>Karen Henderson</td>
</tr>
<tr>
<td>SciQuest - Purchasing**</td>
<td>Carol Kissal</td>
<td>Loette Gossby</td>
<td>Tom Vincent - Integrations</td>
</tr>
<tr>
<td>SOR - Supply Chain Management and AP for EHC</td>
<td>Jimmy Hatcher</td>
<td>Lee Partridge/Gene Harris</td>
<td>Jim Albert</td>
</tr>
<tr>
<td>Southern Treasury Mgmt System*</td>
<td>Carol Kissal</td>
<td>John Hallay</td>
<td>Tom Vincent - Integrations</td>
</tr>
<tr>
<td>Thompson Reuters Tax Advisor</td>
<td>Carol Kissal</td>
<td>Stephen Franges</td>
<td>Karen Hargis - Integrations</td>
</tr>
<tr>
<td>Northern Trust - Endowment Custodial Mgmt System**</td>
<td>Chief Investment Officer</td>
<td>Kristi L. Monsour</td>
<td>Francie Ferdinand/Deapiah Harris/Cede Red</td>
</tr>
<tr>
<td>Wells Fargo Treasury Mgmt System**</td>
<td>Carol Kissal</td>
<td>John Hallay</td>
<td>Tom Vincent - Integrations</td>
</tr>
</tbody>
</table>
**Externally hosted vendor system**

**Policy Details**

1. The EVP, Business and Administration (or designee) must document and maintain a list of all Critical Financial Reporting Systems along with a designated Business Owner, System Owner and Technical Owner for each Critical Financial Reporting System.

2. System Owners in conjunction with system administrators, application administrators, and vendors are responsible for ensuring that Critical Financial Reporting Systems meet or exceed the following minimum standards. These administrative requirements may be waived by the system owner for externally hosted vendor systems when the vendor is unable or unwilling to meet the requirements. All waivers must be documented by the System Owner and communicated to the Business Owner.

   **Access Controls**
   
   i. Initial access rights to Critical Financial Reporting Systems and any subsequent modifications to user rights/permissions must be formally requested and authorized by the appropriate System Owner (or designee).
      a. Authorization of initial access requests and any subsequent requests to modify user rights/permissions must be documented and retained in accordance with Emory record retention policies.
      b. Users are not allowed to authorize their own access requests.
      c. Access rights/permissions should be sufficient to meet the minimum requirements for the user’s role, but not unreasonably exceed the level of authorization necessary to perform legitimate job functions.
   
   ii. If a user’s employment is terminated, the user’s access rights must be promptly removed or disabled. To accomplish this, functional managers and supervisors are responsible for ensuring that terminations are recorded in PeopleSoft HR within 1 business day. Once PeopleSoft HR reflects the termination, system owners are responsible for ensuring that system access changes are processed within 2 business days.
   
   iii. If a user’s job role changes, the user’s access rights/permissions must be reviewed and the user’s access rights must be removed or modified as appropriate. To accomplish this, functional managers and supervisors are responsible for ensuring that job role changes are recorded in PeopleSoft HR within 5 business days. Once PeopleSoft HR reflects the job role change, system owners are responsible for ensuring that appropriate system access changes are processed within 25 business days.
   
   iv. User accounts and permissions must be periodically reviewed to confirm that access rights and permissions associated with the accounts are reasonable and appropriate and do not exceed the level of authorization necessary to perform legitimate job functions. Periodic reviews of all users must occur at least annually. Periodic reviews of users with full access privileges must be reviewed at least quarterly.

   **Segregation of Duties**
   
   i. User accounts, roles, and permissions must be periodically reviewed to confirm that the access rights and permissions associated with the accounts and/or roles are reasonable and appropriate, and that adequate segregation of duties exists to prevent and/or detect fraudulent use of the system. The periodic reviews must occur at least annually.

   **Review Procedures**
   
   i. Procedures must be implemented in support of the above requirements for each Critical Financial Reporting System. System owners may modify this process so long as the modified process is documented and is consistent with the requirements documented above. This requirement may also be waived by the system owner for users with highly restricted access rights (e.g. read only users, users with no access to critical financial functions, users with no access to sensitive data). All waivers must be documented by the System Owner and communicated to the Business Owner.
      a. The system administrator or application administrator will make available to the system owner (or designee) the user accounts, roles, and the permissions/rights associated with each user account and/or role.
      b. The system owner (or designee) will review the list and ensure that permissions/rights associated with each user account and/or role is reasonable and appropriate, and that adequate segregation of duties exists within the system.
   
   ii. Evidence that this review has been conducted will be maintained by the system owner in accordance with Emory document retention policies.
   
   iii. The system owner (or designee) will document any required modifications to permissions/rights associated with any user accounts or roles and communicate the required modifications to functional or technical staff responsible for modifying permissions/rights for the system and to business units that may be impacted by the modifications.
   
   iv. The functional or technical staff will make the requested modifications to permissions/rights.
   
   v. The system owner (or designee) will confirm that the requested modifications have been implemented.
   
   vi. Evidence that this review has been conducted will be maintained by the system owner in accordance with Emory document retention policies.

   **Audit Reports for Externally Hosted Vendor Systems**
   
   i. External vendors hosting Critical Financial Reporting Systems should engage independent auditors to conduct an SSAE 16 SOC 2 Type II review on an annual basis. A copy of the Service Auditor’s Report must be provided to the System Owner within 60 days following the completion of the review. If the external vendor does not, for whatever reason, provide an SSAE 16 SOC 2 Type II report, the System Owner must perform alternate reviews to ensure expected controls are in place to provide similar assurances that would have been provided by the...
SSAE 16 SOC 2 review. This review must be documented and a copy provided to the Business Owner and Emory’s Chief Information Security Officer within 30 days of the last day of the fiscal year.

ii. The system owner must review the SSAE 16 SOC 2 Type II report and provide a copy of the report along with their response to the Business Owner and Emory’s Chief Information Security Officer within 30 days of receiving the report.

E. Compliance
i. Critical Financial Reporting Systems that store, process, or transmit sensitive information that is protected by regulation (e.g. HIPAA, FERPA) or contract (e.g. credit card/cardholder data) must comply with any additional requirements dictated by the governing regulations/contracts.

3. Technical Owners in conjunction with System Administrators, Application Administrators, and vendors are responsible for ensuring that Critical Financial Reporting Systems meet or exceed the following minimum standards. These technical requirements may be waived by the system owner for externally hosted vendor systems when the vendor is unable or unwilling to meet the requirements. All waivers must be documented by the System Owner and communicated to the Business Owner.

A. Anti-Virus Controls
i. Critical Financial Reporting Systems must utilize anti-virus software to protect against malicious code at all times. Exceptions to this requirement must be documented and authorized in writing by the system owner.
   a. Anti-virus software and virus detection signature files must be kept up-to-date.
   b. The system must be configured to automatically retrieve and apply updates to anti-virus software and virus detection signature files at least weekly.
   c. Anti-virus software must be configured to scan files upon access in real-time.
   d. Anti-virus software must be configured to protect the entire file system, but may be limited to file types recommended by the anti-virus vendor.

B. Auditing and Review
i. Audit logs must capture and preserve information needed to detect key events and conditions that might indicate possible fraudulent use of the Critical Financial Reporting System. Key events and conditions to be logged by the system (operating system, application, database, web server, etc.), should include the following whenever possible:
   a. Login attempts
   b. Stopping/Starting of security process or processes that listen on the network
   c. File permission changes
   d. Addition or deletion of user accounts
   e. Modification of user rights or permissions
   f. Changes to system security configurations (e.g. changes to password policy, audit/logging policies)
   g. Attempts to access protected resources (e.g. files, database tables)
   h. Actions taken by administrative users
      i. Privilege escalation events (e.g. su, sudo, run as)
      j. Core system events (e.g. startup/shutdown, system crash, core dump)
      k. Addition, deletion, modification, or viewing of sensitive information
      l. Transactional events that can be used to determine the activities taken by a user (queries executed, changes made, screens viewed, etc.)
   i. For each event the following data elements should be logged if possible
      a. Date and time of the event
      b. User account associated with the event
      c. Description of the event
      d. Success or failure of the event
      e. Source of the event (e.g. IP address, system name)
      f. Event specific details
   ii. Audit logs should be written to write once media, logged to a remote logging server or be copied from the server to backup media or a secure log repository at frequent regular intervals.

C. Authentication and User Identification
i. All Critical Financial Reporting Systems must require each user of the system to authenticate with accounts that uniquely identify the user.

D. Backup and Recovery
i. Data backup procedures to create and maintain retrievable, exact copies of all necessary Critical Financial Reporting System data must be established and implemented.
ii. All removable media used for backing up Critical Financial Reporting System data must be stored in a properly controlled environment in a secure offsite location or separate building from the system hosting the original data and must be transported in a secure manner.
iii. Removable backup media (e.g. tapes, DVDs) containing personally identifiable information must be encrypted.
iv. The data backup procedure must be periodically tested (at least annually) to ensure that Critical Financial reporting System data can be successfully retrieved from backup media.
v. Critical Financial Reporting Systems must also comply with any Emory business continuity and disaster recovery policies.

E. Incident Response
i. If a Critical Financial Reporting System is compromised or suspected of being compromised the incident must immediately be reported to the system owner, central IT Security, and the Chief Information Security Officer.
ii. Fraudulent or suspected fraudulent use of a Critical Financial Reporting System that may have exposed
敏感信息必须立即被报告给系统所有者、中央IT安全和首席信息安全官。

F. Passwords
i. 密码的所有用户账户必须满足Emory的Enterprise Password Policy的要求（http://policies.emory.edu/5.15）。

G. Physical Security
i. 所有关键财务报告系统必须位于物理上安全的区域，并受保护免受未经授权的物理访问。
   a. 入口和出口必须限制，所有访问记录必须维护。

H. Security Updates and Patches
i. 所有关键财务报告系统必须保持与最新的安全补丁和更新同步。合理的认证和部署安全更新的时间是允许的，但部署的时间框架应适合更新的风险水平。
   a. 高风险漏洞的更新应在30天内部署。
   b. 所有更新，包括安全漏洞的更新，应在90天内部署。
   c. 对于任何不能在要求的时间框架内部署的更新，必须制定详细的实施计划。必须在要求的部署时间框架到期前向系统所有者和首席信息安全官沟通这个计划。

I. Segregation of Duties / Change Control
i. 分离职责必须存在，以确保开发或提交关键财务报告系统变更的人士没有权利在未正式批准和监督的情况下将这些变更投入生产环境。
   a. 正式变更管理程序必须为每个关键财务报告系统文档化和实施。
      1. 文档化变更请求
      2. 文档化变更请求的批准由独立于变更请求的监督机构进行
      3. 一个审查过程，以确保未进行未记录的变更，并且所有记录的变更都已得到批准。证据说明这个审查已经由系统所有者按照Emory文件保留政策进行。

J. System Warning Banners
i. 所有关键财务报告系统必须显示一个系统警告横幅，当技术上可行时。横幅上的文本必须说明“你将要访问的计算机系统由Emory University或Emory Healthcare维护或提供，仅供授权用户使用。未经授权的使用将受到刑事处罚。继续使用该系统意味着您接受Emory的IT使用条件和其他适用政策，并同意监控、检索和披露该系统中的任何信息，用于法律执行目的和其他适用的政策。"。

Sanctions:

Failure to comply with this policy may have legal consequences and may result in:

- Suspension or termination of access;
- Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy.

Definitions

I. Business Owner – 业务所有者是负责关键财务报告系统的主要业务功能的业务执行者或领导者。这个角色通常是机构的高级管理层。

II. System Owner – 系统所有者是关键财务报告系统的功能单元领导者，负责关键财务报告系统的正确运行。这个角色负责确保关键财务报告系统满足机构的业务需求，包括遵守与机构相关的政策。系统所有者还负责确定用户适用的适当角色和权限。这个角色通常是关键财务报告系统的高级角色。

III. Technical Owner – 技术所有者是负责确保关键财务报告系统的技术信息组件执行的个人。这个角色负责确保关键财务报告系统的技术信息组件在适当的支持下被正确实施和
managed effectively. Information Technology components may include operating systems, servers, applications, databases, networks, etc. This role is usually a manager or director level IT staff member within either the functional unit or central IT.

IV. System Administrator - The system administrator is the individual responsible for the proper operational configuration, management, and functioning of one or more information technology components of the Critical Financial Reporting System such as an operating system, server, database, etc. This role is usually a staff level IT position within either the functional unit or central IT.

V. Application Administrator - the application administrator is the individual responsible for the proper operational configuration, management, and functioning of one or more Critical Financial Reporting System applications. This role is usually a staff level IT or functional position within the business unit.

Related Links

- Current Version of This Policy: [http://policies.emory.edu/5.11](http://policies.emory.edu/5.11)

Contact Information

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarification of Policy</td>
<td>Chief Information Security Officer</td>
<td>(404) 727-2630</td>
<td><a href="mailto:brad.sanford@emory.edu">brad.sanford@emory.edu</a></td>
</tr>
</tbody>
</table>

Revision History

- Version Published on: Mar 17, 2016 (Updated applications and contacts, other minor changes)
- Version Published on: Mar 17, 2016
- Version Published on: Feb 04, 2009 (Original Publication)

*Emory University policies are subject to change at any time. If you are reading this policy in paper or PDF format, you are strongly encouraged to visit policies.emory.edu to ensure that you are relying on the current version.*