Policy 5.11
Critical Financial Reporting Systems Security Policy

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>AWA – 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 Halley</td>
<td>Tom Vincent – Integrations</td>
</tr>
<tr>
<td>Blackline**</td>
<td>Carol Kissal</td>
<td>John Halley</td>
<td>Tom Vincent – Integrations</td>
</tr>
<tr>
<td>Code Red</td>
<td>Chief Investment Office</td>
<td></td>
<td>Tom Vincent – Integrations</td>
</tr>
<tr>
<td>CORE – Cashlining 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>John Halley</td>
<td>Dana Hargis</td>
</tr>
<tr>
<td>EmoryCard ShielCard</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>Allisyn Berg</td>
<td>Tom Vincent – Integrations</td>
</tr>
<tr>
<td>SE Centricity Business – Patient Billing for Emory Users**</td>
<td>Jimmy Hatcher</td>
<td>Melanie Bruns</td>
<td>Rhoda Dzuric</td>
</tr>
<tr>
<td>Health Quest – Patient Billing for EHC</td>
<td>Jimmy Hatcher</td>
<td>Jim Ferry</td>
<td>Rhoda Dzuric</td>
</tr>
<tr>
<td><em>Pmngrchase Payment Network</em>*</td>
<td>Carol Kissal</td>
<td>Loetitia Gossby</td>
<td>Tom Vincent – Integrations</td>
</tr>
<tr>
<td>Science Timeskeeping System</td>
<td>Carol Kissal/Jimmy Hatcher</td>
<td></td>
<td>Karen Hsiauly/Jen Mezuk</td>
</tr>
<tr>
<td>Thompson Financials</td>
<td>Tom Vincent – Integrations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thompson Financials</td>
<td>Carol Kissal/Jimmy Hatcher</td>
<td></td>
<td>Karen Hsiauly/Jen Mezuk</td>
</tr>
<tr>
<td>Thompson Financials</td>
<td>Carol Kissal/Jimmy Hatcher</td>
<td></td>
<td>Karen Hsiauly/Jen Mezuk</td>
</tr>
<tr>
<td>Thompson Financials</td>
<td>Carol Kissal/Jimmy Hatcher</td>
<td></td>
<td>Karen Hsiauly/Jen Mezuk</td>
</tr>
<tr>
<td>Thompson Financials</td>
<td>Carol Kissal/Jimmy Hatcher</td>
<td></td>
<td>Karen Hsiauly/Jen Mezuk</td>
</tr>
<tr>
<td>SciQuest – Purchasing**</td>
<td>Carol Kissal</td>
<td>Loetitia Gossby</td>
<td>Tom Vincent – Integrations</td>
</tr>
<tr>
<td>SCM – Supply Chain Management and AP for EHC</td>
<td>Jimmy Hatcher</td>
<td>Lee Partridge/Same Harris</td>
<td>Jim Albert</td>
</tr>
<tr>
<td>Thompson Reuters Tax Advisor</td>
<td>Carol Kissal</td>
<td>Stephen Francis</td>
<td>Karen Hsiauly – Integrations</td>
</tr>
<tr>
<td>Northern Trust – Encompassi Endowment Commercial Mgmt System**</td>
<td>Chief Investment</td>
<td></td>
<td>Thompson Reuters – Application</td>
</tr>
<tr>
<td>Wells Fargo Treasury Mgmt System**</td>
<td>Carol Kissal</td>
<td>John Halley</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.

   A. 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.

   B. 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.

   C. 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.

      l. Evidence that this review has been conducted will be maintained by the system owner in accordance with Emory document retention policies.

      c. 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.

      d. The functional or technical staff will make the requested modifications to permissions/rights.

      e. The system owner (or designee) will confirm that the requested modifications have been implemented.

      l. Evidence that this review has been conducted will be maintained by the system owner in accordance with Emory document retention policies.

   D. 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.)
ii. 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
iii. 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
Sensitive information must immediately be reported to the system owner, central IT Security, and the Chief Information Security Officer.

F. Passwords
i. Passwords for all user accounts must meet the requirements established in Emory’s Enterprise Password Policy (http://policies.emory.edu/5.15).

G. Physical Security
i. Critical Financial Reporting Systems must be located in physically secured areas and protected from unauthorized physical access.
   a. Access to facilities housing Critical Financial Reporting Systems must be controlled and records of access to these facilities must be maintained.

H. Security Updates and Patches
i. Critical Financial Reporting Systems must be kept up-to-date with the most current security patches and updates. A reasonable time to certify and deploy security updates is allowed, but deployment timeframes should be appropriate for the level of risk associated with the update.
   a. Updates that address high risk vulnerabilities should be deployed within 30 days.
   b. All updates that address security vulnerabilities should be deployed within 90 days.
   c. A documented implementation plan must be documented for any security updates that cannot be deployed within the required timeframe. This plan must be communicated to the system owner and Chief Information Security Officer before the required deployment timeframe expires.
ii. Only currently supported operating systems and applications may be utilized by Critical Financial Reporting Systems. Software that is not supported with security updates is prohibited.

I. Segregation of Duties / Change Control
i. Segregation of duties must exist to ensure that the individuals developing or submitting changes to Critical Financial Reporting Systems do not have authority to move those changes into production environments without formal approval and oversight.
   a. Formal change management procedures must be documented and implemented for each Critical Financial Reporting System and must include:
      1. Documented change requests
      2. Documented approval of change requests by an authorized oversight body separate from the change requestor
      3. A review process to ensure that undocumented changes have not been made to Critical Financial Reporting Systems, and that all documented changes have been approved
         a. Evidence that this review has been conducted will be maintained by the system owner in accordance with Emory document retention policies.

J. System Warning Banners
i. Critical Financial Reporting Systems must display a system warning banner at each interactive login when technically feasible.
ii. The text of the system warning banner must read “You are about to access a computer system maintained or made available by Emory University and/or Emory Healthcare that is intended for authorized users only. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. By proceeding, your use of this system constitutes your acceptance of Emory’s IT Conditions of Use and other applicable policies and your consent to monitoring, retrieval, and disclosure of any information within this system for any purpose deemed appropriate by Emory University or Emory Healthcare, including law enforcement purposes and enforcement of rules concerning unacceptable uses of this system.”

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 – The business owner is the business executive or leader who is accountable for the primary business functions performed by the Critical Financial Reporting System. This role will usually be a director level or higher role within the institution.

II. System Owner – The system owner is the functional unit leader who is responsible for the Critical Financial Reporting System and its proper functioning. This role is responsible for ensuring that the Critical Financial Reporting System meets the business needs of the institution, including complying with relevant institutional policies. The system owner is also responsible for determining appropriate roles and permissions for users of the system, and for ensuring appropriate use of the system. This role will usually be a director or manager level position within the functional unit responsible for the business functions performed by the system.

III. Technical Owner – The technical owner is the individual who is responsible for ensuring that the technical information technology components of the Critical Financial Reporting System are properly implemented and
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

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.