Policy 5.11
Critical Financial Reporting Systems Security Policy

This policy version was not current at the time of printing. Please see http://policies.emory.edu/5.11 for the current version.

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: February 04, 2009

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 financial reporting.

This policy is effective immediately for new systems. Existing systems have 6 months from the effective date of this policy to fully implement the requirements, unless otherwise noted.

Applicability

This policy applies to all information systems which have been deemed critical for accurate financial reporting (Critical Financial Reporting Systems) by the EVP, Finance and Administration or his 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>A/P</td>
<td>Edie Murphree</td>
<td>Lottie King</td>
<td>Scott Swann</td>
</tr>
<tr>
<td>ACE - Gift/Pledge/Constituent System</td>
<td>Jane DiFalco Parker</td>
<td>Ben Tompkins</td>
<td>Ben Tompkins</td>
</tr>
<tr>
<td>Bank of America Treasury Mgmt System</td>
<td>Edie Murphree</td>
<td>Kim Pate</td>
<td>Scott Swann/Bank of America</td>
</tr>
<tr>
<td>CORE - Cashiering System**</td>
<td>Edie Murphree</td>
<td>Michael Jacubenta</td>
<td>Dana Haggas/CORE</td>
</tr>
<tr>
<td>FAS - General Ledger**</td>
<td>Edie Murphree/Jimmy Hatcher</td>
<td>Belva White/Lynn Johnson</td>
<td>Scott Swann</td>
</tr>
<tr>
<td>GAR - General Accounts Receivable*</td>
<td>Edie Murphree</td>
<td>Michael Jacubenta</td>
<td>Scott Swann</td>
</tr>
<tr>
<td>GE Travel Card System**</td>
<td>Edie Murphree</td>
<td>Lottie King</td>
<td>GE Capital/Amex</td>
</tr>
<tr>
<td>Health Quest - Patient Billing for EHC</td>
<td>Jimmy Hatcher</td>
<td>Rhonda Dozier</td>
<td>Rhonda Dozier</td>
</tr>
<tr>
<td>IDX - Patient Billing for Emory Clinic</td>
<td>Jimmy Hatcher</td>
<td>Jerry Davis</td>
<td>Rhoda Dozier</td>
</tr>
<tr>
<td>MARS - P-Card System**</td>
<td>Edie Murphree</td>
<td>Lottie King</td>
<td>Scott Swann/GE</td>
</tr>
<tr>
<td>OPTIX - Imaging System</td>
<td>Brett Corvell</td>
<td>John Wilson</td>
<td>Valeria Burian</td>
</tr>
<tr>
<td>PeopleSoft Financial Aid</td>
<td>Heather Mugg</td>
<td>Beth Broyles/Dean Bentley</td>
<td>Dana Haggas</td>
</tr>
<tr>
<td>PeopleSoft Financials</td>
<td>Edie Murphree/Jimmy Hatcher</td>
<td>Belva White/Lynn Johnson</td>
<td>Scott Swann</td>
</tr>
<tr>
<td>PeopleSoft HR</td>
<td>Peter Barnes/dailes Howard</td>
<td>Mary Smith/Darlene Wade</td>
<td>Dana Haggas</td>
</tr>
<tr>
<td>PeopleSoft Payroll</td>
<td>Edie Murphree/Jimmy Hatcher</td>
<td>Joleen Mitchell/Manan Oglesby</td>
<td>Dana Haggas</td>
</tr>
<tr>
<td>PeopleSoft Student Financials</td>
<td>Edie Murphree</td>
<td>Michael Jacubenta</td>
<td>Dana Haggas</td>
</tr>
<tr>
<td>PMM - Purchasing and AP for EHC</td>
<td>Jimmy Hatcher</td>
<td>LEE Partridge/Deborah Clement</td>
<td>Rhonda Dozier</td>
</tr>
<tr>
<td>SciQuest - Purchasing**</td>
<td>Edie Murphree</td>
<td>Lottie King</td>
<td>Scott Swann/SciQuest</td>
</tr>
<tr>
<td>SunTrust Treasury Mgmt System**</td>
<td>Edie Murphree</td>
<td>Kim Pate</td>
<td>Scott Swann/Suntrust</td>
</tr>
<tr>
<td>My State Street - Endowment Custodial Mgmt System**</td>
<td>Edie Murphree/Mary Cahill</td>
<td>Belva White/Coleen McMenamin</td>
<td>Scott Swann/State Street</td>
</tr>
<tr>
<td>Travel and Expense*</td>
<td>Edie Murphree</td>
<td>Lottie King</td>
<td>Scott Swann</td>
</tr>
<tr>
<td>Wachovia Treasury Mgmt System**</td>
<td>Edie Murphree</td>
<td>Kim Pate</td>
<td>Scott Swann/Wachovia</td>
</tr>
</tbody>
</table>
Policy Details

1. The EVP, Finance 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. Functional managers and supervisors are responsible for ensuring that terminations are recorded in PeopleSoft within 1 business day. System owners are responsible for ensuring that terminations recorded in PeopleSoft 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. Functional managers and supervisors are responsible for ensuring that job role changes are recorded in PeopleSoft within 5 business days. System owners are responsible for ensuring that job role changes recorded in PeopleSoft 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.
   1. 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.
   1. 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 must engage independent auditors to conduct a SAS 70 (Type I or 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.

ii. The system owner must review the SAS 70 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 should be encrypted if possible. After 9/1/2010 all removable backup media 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 following minimum complexity requirements if technically feasible:
      a. Passwords must be at least 8 characters in length
      b. Passwords must contain at least one uppercase and lowercase character along with at least one number or special character.
      c. Passwords must not consist of your name, NetID, or a word found in a dictionary of any language, and should not otherwise be easily guessable.
   ii. Passwords for all user accounts must be changed periodically. The change interval must not exceed 13 months.

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
         i. 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 an Emory University and/or Emory Healthcare computer system 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 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.”
   iii. Technical Owners in conjunction with System Administrators, Application Administrators, and vendors are responsible

Definitions

1. 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.
2. 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.
3. 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.
4. 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.
5. 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

*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.*