70001.001 Finance Security for ECU Employees

Authority: International Organization for Standardization Standard 27002;
N.C.G.S. Chapter 147, Article 3D;
G.S. §147-33.110;
G.S. §147-33.113;

Related Policy: Information Technology Security and Risk Management Charter;
State of North Carolina Statewide Information Security Manual

Additional References:

https://www.scio.nc.gov/library/pdf/StatewideInformationSecurityManual/Statewide_Information_Security_Manual_April_20_2012.pdf

Reviewed Date: November 27, 2023

Last Revised Date: June 17, 2024

---

1. Purpose: ECU Systems Coordination is responsible for controlling access to the Banner Finance System.

2. Prior to receiving any type of access, users must complete the required training. All users requesting any General Ledger access must complete Banner Finance Training for New Users.

3. System access to the Banner Finance System is requested by logging into the ECU PiratePort portal located at https://pirateport.ecu.edu/connect/ and following the steps listed below.
    a. Users will log into PiratePort using their PirateID and password combination.
    b. Select **Banner Security Request**.
    c. Once in the Banner Security Request, users will select **Request Security** under options.
    d. The correct supervisor of the employee must be listed in the Supervisor Information displayed. Directions to update the supervisor are provided on the form.
    e. Users will choose **Finance** at the bottom of the form, and they will be taken to another screen to select the specific security roles needed to perform their job duties. **User will make selections from the drop-down menus associated with the sub-modules and select submit when done. The user will then be returned to the initial landing page.*
    f. As needed, users should add comments to the Banner Security Request form.
    g. Select access to sensitive data options if necessary.
    h. Select Submit to finalize the request.
    i. Users are required to acknowledge Confidentiality Statements to obtain Finance Security.

4. Finance Security approval routing is as follows:
    a. Employee Submission
    b. Supervisor Approval
    c. Departmental Security Custodian Approval
    d. Sub-module Approver(s) (Determined by the roles selected)
    e. Finance Module Approver
    f. ITCS Security Administration Approver
        i. Users may check the status of their request at any time via returning to PiratePort, Banner Security Request, Request Security and clicking on their most recent request number.

5. When Finance Security is granted, an email notification is sent to the employee and the supervisor listed.
    a. If the request is denied, an email notification is sent to the employee and the supervisor listed.

6. Departmental Security Custodians have knowledge of the duties appropriate for employees within their unit and approve the initial request. For this reason, supervisors who receive a campus-wide finance security reviews should contact their Departmental Security Custodians for assistance in the review and approval.

7. Campus-wide security reviews are performed on a semi-annual basis through ITCS via an ecuBIC report. Changes needed to a staff person's security are submitted to ITCS via Team Dynamix by the appropriate supervisor and once the report for each staff person is correct, the supervisor will click **Approve**. Copies are available for management or auditor review upon request. Systems Coordination will review the response results to determine which remain outstanding. Weekly reminder emails are sent when necessary to ensure all reviews are returned.
    a. Finance security reviews include both security class and organization access.
    b. Internal security reviews are performed quarterly within Systems Coordination. This review focuses on users with modify access to critical Finance functions, edits combinations of security classes for problem situations, identifies users with locked accounts, etc. Logs are maintained within Systems Coordination to document review dates. Departmental follow-up is initiated when needed.
    c. Weekly Finance Security edit reports are monitored to identify security situations outside the normal data expectations.

8. Semi-annual reviews are performed by each of the Sub-Module Approvers. Scheduled reports run on a monthly cycle. Logs are maintained to document the review.

9. SSN Security Review - Effective September 30, 2016, Systems Coordination scheduled FYQG128 to run quarterly. This is an automated SAS program that targets a run date of October 1, January 1, April 1 and July 1. Programmatic emails are sent to the supervisor identified from the ECU.HR_REPORTING_STRUCTURE table for all users with the BAN_GEN_ALLOW_SSN_C class. This quarterly review is managed centrally by Systems Coordination for all Banner Modules. Exception records are provided in the report output located on \\piratedrive\fin-serv\reports\Module_Security\FYQG128. Each Banner security administrator is tasked to review and resolve problems listed for their respective modules. Supervisors are required to send an email to syscoord@ecu.edu confirming SSN access for

their employees is still needed or request removal. Tracking documents are maintained in the above-mentioned folder.

10. Student and Temporary Employees with INB Finance Access Review - Effective February 1, 2017, FYQG12A is an automated SAS program that runs quarterly targeted to run on February 1, May 1, August 1 and November 1. Programmatic emails are sent to the supervisor identified from the ECU.HR_REPORTING_STRUCTURE table for all students and temporary employees with Finance INB security. Exception records are provided in the report output located on \\piratedrive\fin-serv\reports\Module_Security\FYQG12A. Supervisors are required to send an email response to syscoord@ecu.edu confirming the access is still needed or request removal. Tracking documents are maintained in the above-mentioned folder.

11. ITCS Operations Security is responsible for automatically removing all Banner security including Finance access based on the weekly termination reports provided by the ecuBIC team. The Finance module administrator receives a copy of the report but takes no action. Records on the report include terminations from the prior week. Systems Coordination maintains additional reports that run weekly to identify terminated users for additional follow-up to this process. NYWE222 is the weekly report. This report catches terminations with odd data that are not picked up in the normal termination process. ***Security is removed when the Banner HR termination date is reached. Effective February 2, 2017, we are investigating a new report for Operations Security to catch the odd data records.***

12. The Systems Coordination policy and intent is to remove all Finance, third party and general security for Finance users when there is a job change. Confusion with report criteria in the past shows that employees within the same HR Home Org have not been identified in the reports provided. Effective February 2017, action has been taken to update the report criteria to fix this security gap. All module security administrators agree that a total revision by a subject matter expert is needed to increase confidence in the Transfer report results.

13. ECU policy states the direct supervisor is responsible for requesting security removal for transferring, terminated and questionable activity by active employees. Systems Coordination provides instructions to management on how to request security removal for their employees. Emergency requests are managed on behalf of management when no other option is found.

14. User and security class changes are communicated to ITCS Operations Security using the Access Modification for Module Approvers queue in Team Dynamix. https://ecu.teamdynamix.com/TDClient/1409/Portal/Requests/ServiceDet?ID=31722

15. Changes to existing Finance Security classes are managed by the Finance Module administrator with guidance from the Director and Assistant Director of Systems Coordination.

16. Detailed information about Finance System security is documented in the Finance Security Manual and other supporting documents that are maintained by Systems Coordination. Security related documentation is maintained in this location: \\piratedrive\Fin-Serv\Systems-Coordiantion\Security.

17. Access to a Finance ePrint report is tied to a Banner Finance Security class. The access to ePrint is usually granted automatically by the Banner Security Request application based on criteria and specifications established for this purpose.

18. Users granted Finance Security receives access to Banner Finance INB and to Banner Finance Self Service Banner (SSB). Access to ePrint and the Operational Data Storage (ODS) is tied to specific Finance Security roles. Effective April 2023, access to ODS must be requested in the Comment field of the Banner Security Request.

19. The Finance Security Module Approver is available to answer questions and assist with the Finance Security process. Contact Systems Coordination at 737-1144 or 328-2706.

Document Date: 9-6-2013
Updated: 11-27-2023 (LaToya Langford)
Last Update: 06-17-2024