

SYSTEM SUPPORT

1.3.8.2 SECURITY

1.3.8.2.7 SIS+ SECURITY AUDIT

Objective: To ensure SIS+ integrity by removing Student Information Systems access from former employees or employees who have changed departments.

Functional Areas Affected: Registrar's Office Security Officer and all departments with SIS+ users.

Inputs/Source Documents	Screens	Outputs
Focus Security Screens	 002, 005, 012	secaudit.fex (all departments) secaudi2.fex (check list) secaudi3.fex (2 nd request)

The SIS+ Security audit is performed once each year, usually in early June. The following steps should be followed:

1. After logging onto the mainframe, at the dollar prompt enter: proj psis1. At the next dollar prompt, enter: IAFOCUS SHELL/ZS\$.
2. Once in focus' Table Talk, arrow down to "Commands" and select this option. At the focus prompt, enter: TED SECAUDIT.
3. Change the due date in the header and run the report. After the report is printed, discard any pages that are not associated with a real department.
4. Also, run SECAUDI2.FEX to produce the check-off list to keep track of the forms returned and those still out.
5. Print the "Security Audit Labels1" in the Address Label folder on the Admin 167 drive. While some names on the labels will receive multiple pages from the report for multiple departments, the labels should be in order of the pages from the report. This will make stuffing the envelopes easier.
6. Prepare a list for Public Safety manually. It is a group logon. Send the names of those for whom we have Ferpa forms to Mick Smothers, Parking Office. Ask him to write

"DEL" by any person no longer there and to provide forms for any new employees who are accessing the group logon.

7. Stuff the report pages into the campus envelopes and mail.
8. When the signed reports are returned, verify the signature, update the Approved Security Signature list if necessary, and mark the check-off list. If form is not signed by the authorized security supervisor for the area, contact the authorized person to verify that the form may be processed. If approval is not given, destroy the form and send a new form to the authorized security supervisor for the area.
9. Once the first deadline has been reached, review the check-off list. Send a second request for the information to any departments that have not returned the form. (Run SECAUDI3.FEX for the departments that have not returned the forms.) Note: a "FINAL" request may also be necessary for some departments. (Create using SECAUDI3.FEX and changing text in header.) Advise the contact that this is the last request and that SIS+ access will be turned off for everyone by 5:00 pm today unless the signed form is returned by 4:30 pm (or similar).
10. When all forms are returned, go to Security Screen 002 and do a name search for each individual marked as "DEL" on each list. Write down by the name, the department, the operator ID, the user ID, and the templates belonging to the user. All this information is available on Screen 002.
11. After the above is gathered, go to Security Screen 005 and use the operator ID. Start deleting the records. (Note: All operator information will be deleted without asking for confirmation. The deletion is final. Be careful.)
12. After all are deleted, create a Microsoft Table document of those records that were deleted. After entering the records from the lists, sort the table alphabetically. Put instructions at the top for a student worker to pull the forms for the following individuals and return the pulled forms to Donna Van Canneyt, Associate Registrar. These will be held for a time and then shredded.
13. After printing the above for the student worker, change the instructors at the top for Database Systems Programmer II, Rick Roeser, by requesting that he remove the SIS+ Production item from the menu of the following individuals. In the request, ask that Rick let you know when he has completed the task.

NOTE: Wait for two weeks after the deletions from SIS+ security before sending the list to Rick. This will give any that were deleted from the system in error a chance to be corrected before removing the item from their menu.

14. File the returned signed lists, copies of the two tables sent to Rick and given to the student worker, an updated copy of the approved signature list, and the pulled forms to be shredded in a folder labeled "SIS+ Security Audit". Retain until next year's audit.