

Texas A&M University Procedure for FAMIS Security Breaches

Updated 11/16/01

Security Breach - sharing a password or utilizing another's FAMIS access to inquire on data from or input data onto FAMIS screens.

Allegations

- Upon notification of an alleged security breach, FAMIS Security will immediately reset the employee's password and contact him/her with the new password.
- FAMIS Security will notify the department head in writing and copy the senior business administrator. The notification will include an explanation of the allegation, types of access involved, security ramifications, and a copy of the security procedure.
- The department head will either initiate or delegate an investigation of the facts. The department head will submit, in writing, the findings of the investigation to FAMIS Security by a deadline set by FAMIS Security. If FAMIS Security does not receive a response by the deadline, then they will submit a second written notification to the department head and a copy to the senior business administrator expressing the need for a response. If this second notification does not elicit a response, then FAMIS Security will cancel the employee's access until they receive a response.
- If a security breach is documented, then the procedure for First Occurrence should be followed. If no security breach is documented, then no further action is necessary.
- The FAMIS Security Coordinator will keep any appropriate documentation of allegations.

First Occurrence

- The department head will review the allegation with the employee.
- Depending on the severity of the breach, the department head will also determine if any disciplinary action will be taken.
- The first occurrence may result in FAMIS access suspension. The department head will determine the length of any FAMIS access suspension. To ensure consistency in handling security breaches across the university, department heads are encouraged to coordinate with FAMIS Security in determining the severity of the breach and suspension time.
- The department head will notify FAMIS Security explaining the findings of the investigation and actions taken. FAMIS Security will review the department head's decision to ensure consistency in handling security breaches across the university. If the department head's decision does not appear to be in proportion to the severity of the breach, then FAMIS Security will request review by the department head [the senior business administrator will be advised of this request].
- FAMIS Security will notify the Vice President for Finance and Controller if the department does not take appropriate action.
- Other action may be taken in accordance to federal and state law (Chapter 33 Section 1, Title 7 of the Texas Penal Code), depending on the severity of the breach.
- If a security breach is documented, prior to granting access and resetting password, the employee and a witness will sign a paper copy of the FAMIS Statement of Responsibility, which will be filed in the individual's FAMIS security file.

Second Occurrence

- The same procedures for First Occurrence apply to the Second Occurrence.
- FAMIS Security will send a notification of a second occurrence security breach to the following:
 - Department Head
 - Dean or Appropriate Vice-President
 - Assistant Vice-President for Finance
 - Director of Purchasing Services (if the occurrence is in regards to the Purchasing Module)
 - Computing and Information Services Information Technology