Student Services Manual (SSM)

SSM 107–02: Lost, Stolen, or Inappropriately Disclosed Student Records Information

Effective: 1/27/2003 **Revised**: 7/1/2020

Purpose

To provide guidelines for reporting the loss, theft, or inappropriate disclosure of student education records containing personally identifiable information protected from disclosure by the federal *Family Educational Rights and Privacy Act of 1974*, as amended

Sources

Family Educational Rights and Privacy Act of 1974 (also referred to as the Buckley Amendment or FERPA), 20 *United States Code* § 1232g, as amended

University Registrar Services Office of General Counsel

Information Security Office

Policy

Offices, departments, staff, or faculty that experience the loss, theft, or inappropriate disclosure of student education records information are responsible for notifying the police, the individual students, University Registrar Services, the Office of General Counsel and the Information Security Office in a timely manner. Affected departments are also required to develop procedures to avoid future loss, theft, or inappropriate disclosure.

Procedure

Responsibility	**Action**
Office or department reporting loss, theft, or inappropriate disclosure	1. File police report with appropriate jurisdiction, immediately upon detection, if theft has occurred. 2. Report to the Information Security Office (ISO) per the "Incident Response Standard" policy at https://uto.asu.edu/policy/incident-response-standard, when the records theft, loss, or inappropriate disclosure potentially pose a significant risk or could cause significant impact to University systems, assets or personnel. a. ISO will determine if the situation's magnitude, sensitivity and/or computer security warrants additional review by the Incident Response Team. b. ISO must be notified if SSN and/or userids/passwords are part of the data that was lost, stolen or inappropriately disclosed. c. ISO may be required to report certain data breaches or exposures to the Arizona Board of Regents.

	3. Notify the administration office of University Registrar Services and the Office of General Counsel of any loss, theft, or inappropriate disclosure as soon as possible. 4. Draft notification message to all affected students using the approved templates available from University Registrar Services (URS) and submit draft to URS and Office of General Counsel for review and confirmation. 5. Deliver URS and OGC confirmed notification message promptly to all affected students by letter or email. Absent circumstances that warrant a different timeframe, the reporting office or department shall endeavor to provide the notification to the affected students within a week of discovering the loss, theft or inappropriate disclosure. If the disclosed data contained sensitive information which could be used in identity theft or to further compromise the student's records, e.g. SSN, ID numbers/passwords the notification message will advise the student to use one of the following options to monitor any suspicious activities involving possible misuse of information to establish unauthorized credit, etc.: a. Inform student that the Federal Trade Commission (FTC) maintains the U.S. Government's central website for information about identity theft at http://www.consumer.ftc.gov/features/feature-0014-identity-theft b. Certain combinations of loss, stolen or disclosed information may be especially sensitive, leading to the standard practice of also offering complimentary credit monitoring to the affected parties. The cost of this service would be the unit's responsibility. 6. Submit to the administration office of University Registrar Services a copy of the letter sent to students, list of all affected students, and statement indicating proactive steps to be implemented in department to prevent future loss, theft, or inappropriate disclosure of records information.
University Registrar Services	7. Coordinate with the Information Security Office Incident Response Team when the situation's magnitude, sensitivity, and/or computer security issues warrant additional review. 8. Confirm that students and the Office of General Counsel have been notified per policy. Add department's letter, list, and statement to FERPA Violation file and index log. 9. Provide assistance to individual students involved upon request. 10. Consult with department on prevention strategies as needed.

Cross-Reference

For related information, see SSM 203–08, "Affidavit of Dependency for Release of Records."