UNIVERSITY OF PITTSBURGH POLICY 10-02-06

CATEGORY: SUPPORT SERVICES
SECTION: Computing, Information, and Data
SUBJECT: University Administrative Computer Data (UACD) Security and Privacy
EFFECTIVE DATE: January 26, 2018 Revised
PAGE(S): 3

I. SCOPE

This policy establishes data security standards and practices for the protection of University administrative computer data ("UACD") from unauthorized disclosure, and includes the rights and responsibilities of computer data users. It applies to all users of University administrative computer data.

II. POLICY

Protecting University Administrative Computer Data

Computer systems within the University and in the cloud contain information necessary to conduct the business of the institution. This information is defined as University administrative computer data (UACD). Examples include: employee personnel records, student educational records, financial data, and electronic documents, as well as emails used for administrative purposes.

UACD are institutional resources and must be protected from unauthorized modification, destruction, or disclosure, whether accidental or intentional.

It is the responsibility of all levels of management to ensure that all UACD users within their areas of accountability are aware of their responsibilities as established by this policy and for guaranteeing a secure office environment with regard to UACD.

Users of UACD are responsible for:

- Complying with all University computer security and access policies, procedures, and standards.
- Using UACD only as required in the performance of their job functions.
- Disclosing confidential UACD only to other faculty, staff, or students, whose responsibilities require knowledge of such data.
- Exercising due care to protect UACD from unauthorized use, disclosure, alteration, or destruction.
- Adhering to applicable federal and state laws, contractual or grant requirements, and University procedures concerning storage, retention, use, release, transportation, and destruction of data.
- The sharing of passwords and/or use of any University Computing Account is prohibited. You are responsible for all activity performed using your University Computing Account.

Users of UACD are responsible for all transactions occurring during the use of his or her University Computing Account and/or password. A workstation logged into the network with access to UACD must not be left unattended and must be password protected with an idle time-out of no more than 15 minutes implemented.

Personal computers and laptops that access, process, or store UACD must encrypt the hard drives. Also, removable drives such as USB or flash drives must also be encrypted.

If UACD is accessed by mobile devices such as tablets or smart phones, the following must be implemented:

- At least a four-character PIN/password required at power-on or resume inactivity time-out.
- After a maximum of 10 minutes inactivity, the device must require a PIN to be entered for further use (except for answering a telephone call).
- After the entry of 10 consecutive invalid PINs the device will be wiped automatically, preventing further use of the device or access to confidential information.
- All UACD stored on the device must be encrypted.

Access to University Administrative Computer Data

Access to UACD is only permitted to those individuals who are authorized to use UACD as required in the performance of their job functions.

Employees and students may review personal information maintained by the University. Such reviews will be only at reasonable times and only in accordance with University policy and the law. See Policy 07-06-05, Access to Employee Personnel Files; and Policy 09-08-01, Access to and Release of Education Records.

The UACD Data Owner (as identified in University Policy 10-02-04 Computer Data Administration) will confer with University counsel to obtain advice on legal requirements/regulations and the interpretation of privacy laws. The UACD Data Owner will also consult with senior management regarding information access to University data and with CSSD Security regarding methods, technology, processes, and procedures to meet the requirements.

Reporting Violations of Data Security Policy

Violations of this policy should be immediately reported to CSSD Security abuse@pitt.edu). CSSD will consult with Human Resources and the Office of General Counsel as appropriate. The University strives to maintain confidentiality to the extent possible consistent with other obligations.

Disciplinary Action

Violations of this policy will result in appropriate disciplinary action, which may include loss of computing privileges, suspension, termination, expulsion from the University, and/or legal action.

Violations of any federal, state, or local law concerning the unauthorized access or use of University computers and computing services will result in the appropriate disciplinary action up to and including termination from the University.

III. REFERENCES

Policy 07-06-05, Access to Employee Personnel Files

Policy 09-08-01, Access to and Release of Education Records

Policy 10-02-04, Computer Data Administration

Policy 10-02-05, Computer Access and Use