**UNIVERSITY OF PITTSBURGH POLICY 10-02-04**

**CATEGORY:** SUPPORT SERVICES
**SECTION:** Computing, Information, and Data
**SUBJECT:** Computer Data Administration
**EFFECTIVE DATE:** January 26, 2018 Revised
**PAGE(S):** 2

## I. SCOPE

This policy establishes the responsibilities for collecting, maintaining, regulating, and requesting online access to University computer data. It applies to all departments and responsibility centers requiring the use of University computer data.

## II. POLICY

Integrity and Availability of University Computer Data

University computer data is defined as any information stored on a University owned and maintained computer system. This includes data processed or stored on computer hard disks, computer tapes, memory devices, optical disks, any other type of computer data storage media, and cloud storage or systems.

Responsibility for collecting and/or processing accurate and complete University computer data rests with University departments and responsibility centers that have ownership of data stored on University computer systems.

Designation and Responsibilities of a Data Owner

Ultimate data ownership legally rests with the University. Departments and responsibility centers must designate a "Data Owner" that will be a steward of University data and be responsible for:

- Maintaining documented records describing the storage location, the use, and the protection of University computer data. This includes, but is not limited to, creating and maintaining an inventory of data used by the department or responsibility center, documenting users who have access to this data, and documenting controls used to protect this data.
- Addressing the accuracy and completeness of University computer data.
- Ensuring the availability of University computer data through the use of data backup solutions.
- In coordination with department administrators, resolving all discrepancies regarding University computer data concerning an individual (student, faculty, and staff).
- Reviewing and, if appropriate, approving requests for access to University computer data in accordance with Policy 10-02-06, University Administrative Computer Data (UACD) Security and Privacy.
- Establishing and maintaining standards regarding the collection access, maintenance, use, dissemination, and protection of University computer data. These standards must comply with University policies involving computer data.
- Strictly adhering to University policies, guidelines, and procedures that govern distribution, electronic sharing, or storing University data — by any means — outside of the University.

- Ensuring that submitted requests for access to University computer data include the specific computer data required and the purposes for which it will be used.

- A Data Owner may rely on the expertise of an information technology professional to meet these requirements; however, the Data Owner is responsible for ensuring that these requirements are fully addressed.

- A Data Owner may be responsible for all data used by a department or responsibility center, or for specific data sets. Multiple Data Owners may be designated by a department or responsibility center to address multiple data sets within their areas of responsibility.

Authorized Access to University Computer Data

University computer data are considered proprietary information and will be made available on a need-to-know basis to individuals requiring knowledge of such data to perform their job responsibilities. Data Owners are responsible for verifying the access requirements of their staff, and for ensuring that all University computer data users within their areas of accountability are aware of University policies applicable to maintaining the integrity, availability, and confidentiality of University computer data.

It is the responsibility of the requestor to affirm that the accessed University computer data be used only as required in the performance of his/her duties.

Requests which are denied by the Data Owner may be appealed to the appropriate senior officer for consideration.

Reporting Violations of Computer Use Policy

Violations of this policy should be reported immediately 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 10-02-05, Computer Access and Use

Policy 10-02-06, University Administrative Computer Data (UACD) Security and Privacy