Enrollment Systems
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, Pennsylvania 15213-3890

STUDENT DATA AND SYSTEMS SECURITY POLICY

MAINTAINING THE CONFIDENTIALITY OF RESTRICTED DATA

In the course of accessing data or information, you will access restricted information within particular databases.

These databases include, but are not limited to, the S3 applications (S3, SIO, BnA, MPS), (Stellic) Academic Audit, (SDW) Student Data Warehouse and Dining databases, as well as databases held in the Career Center and in Student Health Services. It is the responsibility of the Data Owner* to ensure that all individuals with access to data are aware of the confidential nature of the information and the limitations, in terms of disclosure, that apply.

• When accessing restricted information, you are responsible to maintain its confidentiality without exception. If restricted information is released to you, you will maintain the confidentiality of that data and will not pass the information on to a third party without express permission from the Data Owner*. If a user id and password are granted to allow access to sensitive or restricted data, confidentiality over this data must be maintained.

• The release of restricted information without the express approval of the Data Owner* or outside the guidelines established for such data is strictly forbidden.

• Unauthorized release of restricted information will result in appropriate disciplinary action, including possible dismissal. All matters involving university employees will be reviewed with the Director of Human Resources and /or the Provost. Matters involving students will be reviewed with the Dean of Student Affairs. Matters involving individuals not affiliated with the university will be reviewed with the university attorney.

PROTECTING AND MANAGING PASSWORDS

Passwords are a critical component to any computer security program. To properly control passwords and maintain their integrity, the guidelines below should be followed:

• Passwords should change every 90 days, or more frequently in cases of user ids with access to sensitive or restricted data.

• Users must never give out their personal password to anyone. The sharing of passwords is a violation of this policy.

• As part of the educational process, the Data Security Officer* will provide users with guidelines for selecting and changing their passwords.

_____

I have read and understand the Student Data and Systems Security Policy.
Name _____ User ID _____
Department _____ Phone _____
Signature _____ Date _____
Please make a copy and return signed document to:

Enrollment Systems
Cyert Hall 111

*Definitions for these terms, and additional information on the Official Carnegie Mellon Data Security Policy are located at http://www.cmu.edu/iso/governance/policies/information-security.html

rev:18-aug-2017