Drexel University
Administrative Information Systems

System Owners, System Administrators/Analysts, System Custodians and End Users

Information Security Policy

I. STATEMENT OF PURPOSE:

Drexel University (hereinafter referred to as "the University") is the ultimate owner of all data residing in all Administrative Information Systems. Administrative Information Systems include the Banner System, SCDCOnline, OVT, Web*Finance, Web*Salary, NOLIJ, Exeter and the Institutional Advancement System. All institutional data, whether maintained in an Administrative System or accessed via the Reporting system or copied into other applications and/or computers, remains the property of the University and as such are governed by this policy statement. All levels of administrative management must ensure that, for their areas of responsibility, each system user knows his or her responsibilities as outlined in this policy. Each employee, who uses the Administrative System, prior to accessing the system, must read, understand and indicate their acceptance of this policy.

All **information residing on the Administrative System is considered confidential** and is intended exclusively for purposes related to the University's programs. All of the University's Administrative information should be used only for the legitimate business of the University and specifically not for commercial, personal and/or political purposes.

II. DEFINITIONS:

The **system owner** is a senior vice president in each of the respective areas who represents the University in regards to overall system functionality and leadership within their respective module(s). The **system administrators/analysts** in each of the respective areas work directly for the system owners and are responsible for the overall functionality, accuracy, integrity and security of data within their respective module(s). **Custodians** of the data are responsible for the day-to-day information management including data creation and maintenance. The custodians ensure the ongoing timeliness and accuracy of data entry related to their respective module. Together, the **system administrators/analysts and custodians** ensure the relevance and consistency of data between and among the multiple offices operating on the Administrative Systems within the University. They must create and maintain a secure office environment with regard to electronic data. A list of system owners, system administrators/analysts and custodians for each Administrative module may be found here on the web. The **end user** is anyone accessing the University's Administrative Information System.

III. REQUIREMENTS AND PROCEDURES:

Requests for access to Administrative information, including maintenance and/or inquiry, should be given to the system administrator/analyst who will determine the validity of the request. If the request for access is approved, the system administrator/analyst will authorize, in writing, to the Core Administrative System group of the Office of Information Resources and Technology to

grant permission for the access. If a request for access crosses Administrative modules, the system administrator/analyst for each respective module must review and authorize the request for their respective areas. By approving end-user access, the system administrator/analyst validates that access to the Administrative information is job-related and necessary to perform the duties expected. System Administrators/Analysts reserve the right to deny requests based on their findings. Denied requests for information may be appealed in writing to the system owner.

Data access is provided to end users so that they can more effectively perform the duties of their position. An employee, who is granted access to the Administrative System, must receive general system training supplemented by specific instruction from the system administrator/analyst and/or the custodian of the respective area. This specific training ensures that the end user understands how to interpret the information being accessed. The training should match and not exceed the level of access approved.

Each **end user will be held responsible for the security, privacy and confidentiality of the information to which they have access**. Each end user is responsible for all transactions occurring during the use of their login and password. **End users must never share their passwords with others.** If an end user suspects that their password has been compromised, he/she must immediately change their password to the appropriate Administrative System. End users should logoff of the Administrative System when they are leaving their desk for more than 30 minutes. Data should never be left on any system that does not reside in a controlled area.

All end users are expected to comply with all of the terms and conditions as set forth in this document. Failure to do so may result in denial of access to information in the Administrative System and depending upon the action taken, may lead to disciplinary action up to and including immediate termination.

Any problems or errors in regards to the Administrative System dealing with security, access, functionality, training, or incorrect or suspect data must be reported to the appropriate system administrator/analyst immediately.

IV. **ACCEPTANCE:**

You will be required to electronically register your acceptance of this document to acknowledge that you have read and understood the policies outlined in this document. By indicating your acceptance to this document you are indicating your agreement to accept all of the terms and conditions, as set forth above, as it pertains to use of the University's Administrative system.

By signing and dating this document you fully understand the implications and responsibility you have in regards to Drexel University's Administrative Information and requires a personal commitment to the highest level of honesty and integrity.

Signature and Date

Printed Name

University Id