Access to and Responsible Use of Data

Category: Operations
Responsible Department: Information Services
Responsible Officer: Vice President, Information Services
Effective Date: 11/1/2017

Policy Summary

This Policy explains the processes and requirements for accessing and using (including security) University data.

Scope

This policy affects the following groups of the University:

- Entire University Community

This policy applies to all members of the University Community.

Policy

DePaul University data are a University resource of significant importance and value. Much of the data are confidential and/or sensitive. Therefore, they must be accessed and used appropriately, and protected from unauthorized use and access. The University's policies and procedures for data access and use (including security) serve to ensure that relevant data are accessible for the effective management and legitimate educational and business purposes of the University, while protecting data integrity, providing appropriate data confidentiality, and safeguarding individual privacy. This policy applies to DePaul University data and systems whether they are hosted on DePaul computer systems or outsourced to a third party.

All individuals who access and use University data will be held responsible for adhering to this Policy. Individuals accessing and using specific categories of University data should also consult the relevant policies governing the use of that data.

For example:

- individuals accessing and using student educational record information should consult the various University policies and procedures regarding the Family Educational Rights and Privacy Act (FERPA), and

- individuals accessing and using protected health information should consult the Health Information Privacy Policy regarding Health Insurance Portability and Accountability Act (HIPAA) covered data, and relevant department policies.

Additionally, individuals who desire access to some categories of University data, as defined below, will be required to obtain appropriate management-level approval for access and sign a PeopleSoft Access Request Form or other appropriate request form.

Definitions and Terminology:

Users: A User is any person, authorized or unauthorized, who has electronic or other access to Data. For purposes of this Policy, a User does not include a student or employee who accesses or modifies their own Data for legitimate purposes, for example by using authorized self-service capabilities.

Data: Data are representations of information, knowledge, facts, concepts or instructions. They are considered property and may be in any form including, but not limited to paper, electronic, magnetic or optical storage media, including any storage device used to capture data or data stored internally in the memory of the computer. For purposes of this Policy, Data refers to Data created, held or otherwise owned by DePaul University or its employees for the purposes of conducting DePaul business, education, or research.

Privacy: Privacy is the right of individuals to control personal information about themselves.

Confidentiality: Confidentiality is the state of Data being kept private and secure.

Data Stewards: A Data Steward is a University employee who has been granted responsibility for managing designated Data and/or Data resources in his or her functional area. In conjunction with Information Services (including the Director of Information Security), a Data Steward is responsible for Data acquisition, maintenance, interpretation and definition, application of business rules, integrity and security, and application of access rules. Additionally, Data Stewards must comply with any government regulations covering the data they manage.

All DePaul systems using non-public data must have appropriate Data Stewards assigned.

For research conducted by DePaul employees, wherein DePaul stores the data, the research Principal Investigator or responsible project faculty member or staff person shall be considered the Data Steward. Protection of this data shall be performed according to all applicable laws, project contractual agreements and DePaul protection standards. Data Stewards of research projects should consult with Information Security if assistance is needed.

NetAdmin: NetAdmin is the group within Information Services responsible for implementing and managing requests for access, and requests for removal of access, from the Data Stewards for PeopleSoft and several other systems that are centrally managed by Information Services in accordance with this Policy.

Data Classification

Pursuant to this Policy, there are five categories of Data: Highly Sensitive, Sensitive, Internal Restricted, Internal Non-Restricted and Public. The Security Classifications and Controls matrix, located in the appendices, contains requirements on how individual data elements and classification categories, in general, must be protected.

(1) Highly Sensitive Data. Highly Sensitive Data is Data that is not available within the University without specific authorization. Highly Sensitive Data has Confidentiality and Privacy considerations. A breach of security involving Highly Sensitive Data could lead to serious legal or public relations consequences for the University (either because of statutory rules, contractual obligations, or both) or to serious personal injury for an individual. Examples of Highly Sensitive Data include, but are not limited to: social security numbers, credit/debit or bank account numbers, and driver's license or other state identification numbers and information covered by the Health Insurance Portability and Accountability Act of 1996. .

(2) Sensitive Data: Sensitive data is data that should be assigned to users on a strict business-need basis because it contains personal information of a generally confidential nature, which requires strict handling to protect the privacy of individuals in the DePaul community, but does not have the same risks as Highly Sensitive Data. A breach of Sensitive information could lead to loss of privacy for individuals. Examples of Sensitive Data include health information not covered by HIPAA, statements of assets and/or liabilities, passport and citizenship information and other fields noted in the Security Classifications & Controls Matrix.

(3) Internal Restricted Data: Internal Restricted Data is Data that is available within the University or to others with legitimate business purposes with specific authorization from the appropriate Data Steward. Internal Restricted Data often has Confidentiality and Privacy considerations. Examples of Internal Restricted Data include, but are not limited to: employee pay rates, employee ages, ethnicity, student financial aid, and academic performance information (such as grades, GPA, or academic status).

(4) Internal Non-Restricted Data: Internal Non-Restricted Data is Data that is generally available within the University without specific authorization. Examples of Internal Non-Restricted Data include, but are not limited to: employee names, DePaul telephone numbers and email addresses (not otherwise publicized), employee job titles and dates of employment, internal announcements, and class information not otherwise publicized.

(5) Public Data: Public Data is Data to which the general public may be granted access without restriction. Public Data is not Confidential in any way. Public Data includes Data that DePaul would like presented to the public and Data which is publicly available. Examples of Public Data include, but are not limited to: Data posted on University bulletins and Data on unrestricted University Web sites.

Access to Data

Access to Data is based on the principle of "need to know." Data, including but not limited to Data in DePaul's information systems, data warehouse, network file servers and other databases or downloaded Data, will be made available to Users only for the legitimate educational and/or business purposes of DePaul University.

Access to Public Data & Internal Non-Restricted Data: In general, all members of the DePaul community shall have access to Public Data and Internal Non-Restricted Data without restriction.

Access to Internal Restricted. Sensitive & Highly Sensitive Data: Access to electronic Internal Restricted Data, Sensitive and Highly Sensitive Data shall be granted only by the written authorization of the appropriate Data Steward and upon completion of a PeopleSoft Access Request Form, or other appropriate request form, with certification from the employee's supervisor and an additional designated reviewer. The Access Request Form must specify the scope and purpose for access and proposed uses for the Data. Once access is approved, the supervisor is responsible for overseeing the employee's appropriate use of the Data. In general, access will be granted only for legitimate educational and/or business purposes (i.e. necessary for the User to perform appropriate tasks as specified in a position description or by contractual agreement and/or used within the context of official University business and not for purposes extraneous to the individual's position description or area of responsibility to the University).

Access by Student Organizations: Access to Data by University-recognized student organizations or by individual students who are not student employees shall be granted only with the written authorization from the Dean of Students or his/her designee and the appropriate Data Steward, and upon completion of the appropriate Access Request Form.

User IDs and Passwords: Upon appropriate approval and completion of the appropriate Access Request Form, the appropriate Data Steward in conjunction with NetAdmin or other appropriate administrative functions, will grant access to the User for the Data. User IDs for Data and system access and a corresponding password are assigned to individual DePaul community members. Users must not share their password with any other individual, and no employee of DePaul shall request the password to another individual's user ID. Passwords are a minimum of eight characters in length; and must contain letters, and at least one numeric digit and one special character. Passwords can be changed at any time, but must be changed at least once every 365 days. It is recommended that users with access to confidential data change their passwords at least once every 90 days. By accepting access to Data or by signing the appropriate Access Request Form, the User agrees to maintain the Confidentiality of the Data and the password in accordance with this Policy, including protecting the password from unauthorized use. Users agree to promptly report any incident involving the Confidentiality of their password or suspicion that the Confidentiality of the password has been compromised to the Director of Information Security.

Responsible Use of Data

Data shall be used only for legitimate educational or business purposes. Data should generally be used for the purposes for which they are maintained. Users are expected to respect, and take all necessary steps to protect, the Confidentiality of Data and Privacy of individuals as appropriate and required by the Data Classification or otherwise required. Users are required to abide by any applicable University policies, ethical or professional rules, or legal restrictions governing access to or use of any particular Data.

Unauthorized Use: The disclosure or distribution of Internal Non-Restricted, Internal Restricted, Sensitive and Highly Sensitive Data, in any medium, except for legitimate educational and/or business purposes is expressly prohibited. Access to or use of Data for personal gain or profit or for the personal gain or profit of others is also prohibited. Under no circumstances may any Internal

Non-Restricted, Internal Restricted, Sensitive or Highly Sensitive Data, including but not limited to Data in the DePaul's information systems, files and data warehouse or other databases or downloaded data, be made available to parties external to the University for anything other than legitimate educational and/or business purposes and must have the approval of the appropriate Data Steward and, in the case of Highly Sensitive Data, the Director of Information Security.

Protection from Unauthorized Access and Use: Users shall use reasonable and appropriate means to protect all Data under their control or possession from unauthorized access or use. This includes protecting Data that is archived, and disposing of Data in a responsible manner appropriate to the Data Classification. Users shall promptly report any suspected unauthorized use of Data to the Director of Information Security. Users should consult the "Security Classifications & Controls Matrix" (attached as an appendix hereto) to gain an understanding of "best practices" for protecting Data from unauthorized use.

Administering User Access:
Data stewards must have formal processes for the administration of user access to the data under their responsibility. At a minimum, these processes must include:

- **Granting Data Access to Others:** Data Stewards may receive requests to provide Data or access to Data to others. They may grant such access only as authorized and in accordance with this Policy or other relevant University policies. Data Stewards who grant access must maintain copies of the appropriate Access Request Form in their records according to the Record Retention schedule. These records must be made available to the Director of Information Security or others authorized to review the records upon request. All data access requests must be made through an Access Request Form. Data Stewards are responsible for developing an appropriate Access Request Form for systems they manage if the access is not granted through the PeopleSoft Access Request Form. Access request forms must contain, at a minimum: full employee information (name, employee ID number and user name) for user to be authorized, description of access requested (including explicit mention of any highly sensitive information requested) and business purpose for the access, supervisor information of approving supervisor, Data Steward information of approving Data Steward and date of request. Access requests must be signed by the appropriate supervisory party, the Data Steward, and the employee. The employee signature must certify that the User agrees to maintain the Confidentiality of the Data and the password in accordance with this Policy, including protecting the password from unauthorized use.

- **Terminating Access to University Data:** Once a person is no longer employed in a position that requires access to Data (due to employment termination, transfer, change of job duties, or other event), his/her access must be promptly removed. (Refer to the Termination Process Checklist for more information. Additionally, a person may be removed from access to Data at any time as determined by the Director of Information Security, Data Steward and/or appropriate supervisor/manager.

  The individual's supervisor/manager is responsible for notifying the Data Steward of an employee's change in job status, official roles or responsibilities that result in changes in requirements of access to Data. This information must be relayed to NetAdmin in terms of what access must be changed. Additionally, Human Resources shall provide notice to NetAdmin of any change in job status including, but not limited to termination in a timely

manner. NetAdmin shall be responsible for effectuating access changes to PeopleSoft systems.

- **Reviewing User Access:** Assignments of access to data must be reviewed on a periodic basis, at least annually or at least twice annually for data that is classified as Sensitive or Highly Sensitive. The review should consist of reconfirmation of users ongoing need to retain access to data. If a user's job function has changed, access should be revoked. Documentation of review and sign-off of reconfirmation must be retained.

Reviews of access must be performed for data residing in DePaul information systems, data warehouse, network file servers, or other databases or file systems, including those hosted by an external vendor.

Instructions to review DePaul network file server access can be found at the appendix below.

Violations
Unauthorized access or use of Data is a violation of University policy. All users, but most especially Data Stewards, are required to report any noted violations to the Director of Information Security. Violations of University policy may subsequently be referred to the Dean of Students, and/or Human Resources, as appropriate. Violations may result in appropriate disciplinary measures up to and including termination or dismissal from the University. Student, faculty and employee rights and responsibilities can be found in the appropriate Handbooks or policy. Violations of this Policy may also be a violation of law and may be referred to federal, state and/or local authorities.

Procedures

Specific procedures for implementing this Policy are available from Information Services and from the appropriate Data Steward(s).

Divisional Collaborations

- Human Resources
- Student Affairs
- Financial Affairs
- Internal Audit
- Office of General Counsel
- Information Services Security Team
- Office of the University Registrar
- Enrollment Management
- Financial Aid
- Student Financial Accounts
- Records Management

Contact Information

Information Services
(312) 362-8200

Appendices

Please find attached the following documents:

- PeopleSoft Access Request Form
- Security Classifications and Controls Matrix

Review network file server permissions instructions Windows7:
https://offices.depaul.edu/is/security/Documents/Win7_Search_ADGROUPS.pdf

Review network file server permissions instructions - Windows 8:
https://offices.depaul.edu/is/security/Documents/Win8_Search_ADGROUPS.pdf

History/Revisions

Origination Date:
Last Amended Date:
Next Review Date: