Security Classifications & Controls Matrix for Highly Sensitive, Sensitive, Internal Restricted, and Internal Non-Restricted Covered Data

Note—This Matrix brings together the Data Classifications from the "Access to and Responsible Use of Data Policy" and the notion of Covered Data from the "Information Security Policy".

Data Classification	General Description of Access	
Highly Sensitive	*Highly Sensitive data is data that should be secured with the highest level of protections. A breach of security with respect to Highly Sensitive data could lead to serious legal consequences for the University (either because of statutory rules, contractual obligations, or both) or to serious personal injury or privacy violation for the individual.*	
	Controls for Electronic Data	• Highly sensitive data may only be stored on DePaul's network file servers (specifically, the U: and W: drives), on DePaul's instance of Microsoft OneDrive (depauledu.sharepoint.com or depauledu-my.sharepoint.com), or on third party applications approved by the Information Security team within Information Services. This data is not approved for storage in any other locations unless written authorization is granted by the data owner and University Privacy Officer or their designee. • Highly sensitive data that are approved for storage in other locations must always be encrypted both at rest and in transit using methods approved by the Information Security team within Information Services. If external media are approved, disposal or re-use of such media is prohibited until the media is wiped. • Authorization should be required before access is granted and audited periodically thereafter. Authorization should be requested and granted using standard processes (where they exist) such as the IS Service Request in Campus Connect and the Network Folder Request form in the Help Desk portal. • Only DePaul-issued and managed computers are authorized for use in accessing highly sensitive data, and employees should practice good security hygiene with their DePaul computers, including locking the screen when not in use. Accounts (especially administrator accounts) with access to highly sensitive data or the ability to communicate via e-mail with large populations must use DePaul single sign-on (SSO) and be secured with BlueKey MFA. If this is not possible with a specific application, the application must use a vendor-provided MFA solution to secure administrator accounts, and such accounts must meet or exceed University password requirements. All controls for data of lower classifications also apply to highly sensitive data.
	Controls for Non-Electronic Data	• Data is stored in locked cabinets or in locked rooms with a limited number of keys. Keys are controlled by appropriate departmental personnel and regularly inventoried. • When in use, data is under the direct control of an authorized employee (or otherwise reasonably secured). • Employees with authorization to access data undergo security training prior to receiving authorization. • Data is shredded using bins provided by the Records Management department when disposed of.

<table>
<tr><td rowspan="3">Sensitive</td><td colspan="2">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. A breach of Sensitive information could lead to loss of privacy for individuals.</td></tr>
<tr><td>Controls for Electronic Data</td><td>• Sensitive data may only be stored on DePaul's network file servers (specifically, the U: and W: drives), on DePaul's instance of Microsoft OneDrive (depauledu.sharepoint.com or depauledu-my.sharepoint.com), or on third party applications approved by the Information Security team within Information Services.
○ Sensitive data stored elsewhere must be encrypted both at rest (using full-disk or file-level encryption) and in transit, no matter where it is stored or transmitted (e.g., desktop/laptop computer, server not managed by Information Services, CD/DVD/USB media). Such storage locations must be securely wiped before reuse or disposal.
○ Sensitive data stored and/or transmitted using other methods must also be tracked and documented by the owning department, and documentation must be kept up to date.
• Authorization should be required before access is granted and audited periodically thereafter. Authorization should be requested and granted using standard processes (where they exist) such as the IS Service Request in Campus Connect and the Network Folder Request form in the Help Desk portal.
• Only DePaul-issued and managed computers are authorized for use in accessing sensitive data, and employees should practice good security hygiene with their DePaul computers, including locking the screen when not in use. Accounts (especially administrator accounts) with access to sensitive data or the ability to communicate via e-mail with large populations must use DePaul single sign-on (SSO) and be secured with BlueKey MFA. If this is not possible with a specific application, the application must use a vendor-provided MFA solution to secure administrator accounts, and such accounts must meet or exceed University password requirements.

All controls for data of lower classifications also apply to sensitive data.</td></tr>
<tr><td>Controls for Non-Electronic Data</td><td>• Data is stored in non-public areas which require DePaul Blue Demon Cards, door codes, and/or keys to enter. Blue Demon Card access, door codes, and/or keys are controlled by appropriate departmental personnel and regularly audited.
• When in use, data is under the direct control of an authorized employee (or otherwise reasonably secured).
• Employees with authorization to access data undergo security training prior to receiving authorization.
• Data is shredded using bins provided by the Records Management department when disposed of.</td></tr>
<tr><td rowspan="3">Internal Restricted</td><td colspan="2">Internal Restricted data is data that should be secured with a moderate level of protections.</td></tr>
<tr><td>Controls for Electronic Data</td><td>• Authorization is required to access data. Authorization is given only for business purposes.
• Employees with authorization to access data undergo security training prior to receiving authorization.</td></tr>
<tr><td>Controls for Non-Electronic Data</td><td>• Data is stored in reasonably controlled areas with limited access.
• When in use, data is under the direct control of an authorized employee (or otherwise reasonably secured).
• Employees with authorization to access data undergo security training prior to receiving authorization.
• Data is shredded using bins provided by the Records Management department when disposed of.

All controls for data of lower classifications also apply to Internal Restricted data.</td></tr>
</table>

Internal Non-Restricted	*Internal Non-Restricted data is data that, generally, does not need to be strictly secured within the DePaul community; but that may only be used outside the DePaul community for legitimate educational and/or business purposes.*	
	Controls for Electronic Data	• All employees are trained annually with respect to DePaul policies & procedures regarding misappropriation of data for non-business uses and are trained with respect any other uses that conflict with stated DePaul policies & procedures.
	Controls for Non-Electronic Data	• All employees are trained annually with respect to DePaul policies & procedures regarding misappropriation of data for non-business uses and are trained with respect any other uses that conflict with stated DePaul policies & procedures.
Public	*Public data is data to which the 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*	
	Controls for Electronic Data	• None
	Controls for Non-Electronic Data	• None.

Type of "COVERED DATA"	**Security Classification**	**Additional Specific Controls** *(May be for electronic or non-electronic versions of the "COVERED DATA")*
Social security numbers and partial social security numbers	Highly Sensitive	• Systems and applications that must store full Social Security numbers (SSNs) must mask all except the last four digits when displaying them to end users. Full/unredacted SSNs should never be printed out.

Credit card numbers / Debit card numbers	Highly Sensitive	• Customer credit cards must never be stored anywhere and may not be processed or transmitted using DePaul computers or network. All departments wishing to accept credit card payment must discuss compliance and security requirements with Treasury and Information Security and prepare yearly Payment Card Industry Data Security Standards compliance documentation.
		• For internal DePaul credit card information:
		  ○ Card Security code (also known as CVV - last three numbers on the back of the card) must never be stored
		  ○ Full credit card numbers must never be stored.

Bank account numbers	Highly Sensitive	
Passwords, pins, certificates, and similar data that permit access to DePaul systems, financial accounts or other personal data	Highly Sensitive	• May not be used in report files. • Passwords and pins must never be stored in an unencrypted/plain text format. • May not be stored unencrypted/in plain text within applications, configuration files, APIs, etc.
Driver's license numbers	Highly Sensitive	
State (and other government) identification card numbers/information	Highly Sensitive	
Health Insurance Portability and Accountability Act (HIPAA) covered data	Highly Sensitive	• HIPAA covered data must be encrypted as highly sensitive data requires, must be encrypted if sent externally and during electronic transmission internally. • If we provide PII and/or sensitive data either individual files should be encrypted or all files should be put into an encrypted archive prior to sending/uploading outside DePaul.

Health-related information not covered by HIPAA including student-athlete injury and rehabilitation data, and any other person's health care or health care payment information)	Sensitive	• Must be encrypted if sent externally and during electronic transmission internally.
Passport and citizenship information (including passports of other countries)	Sensitive	
Income and credit information	Sensitive	• To be treated as Highly Sensitive if includes any Highly Sensitive data
Tax returns	Sensitive	• To be treated as Highly Sensitive if includes any Highly Sensitive data
Statements of assets and/or liabilities	Sensitive	
Student financial aid data which contains confidential information such as income information, amounts of loans or grants, repayment status or other information generally considered private	Sensitive	• To be treated as Highly Sensitive if includes any Highly Sensitive data
Confidential Employee Relations Data – data which should be considered private as it may relate to personal employee issues	Sensitive	
Salary information	Sensitive	To be treated as Highly Sensitive if includes any Highly Sensitive data
Research data and advising/counseling data containing sensitive personally identifiable information	Sensitive	To be treated as Highly Sensitive or Internal Restricted if includes any Highly Sensitive or Internal Restricted data
Personal demographics such as birthdate, race, gender, ethnicity, national origin	Internal Restricted	
Other loan information	Internal Restricted	• To be treated as Highly Sensitive or Sensitive if includes any Highly Sensitive or Sensitive data
Scholarship application materials	Internal Restricted	• To be treated as Highly Sensitive or Sensitive if includes any Highly Sensitive or Sensitive data
Donor/potential donor information	Internal Restricted	• To be treated as Highly Sensitive or Sensitive if includes any of these types of data
Payroll information (including benefits information)	Internal Restricted	• To be treated as Highly Sensitive or Sensitive if includes any Highly Sensitive or Sensitive data
Other personally identifiable financial information not otherwise publicly available	Internal Restricted	• To be treated as Highly Sensitive or Sensitive if includes any Highly Sensitive or Sensitive data
Student grades	Internal Restricted	
Other student information on athletic compliance forms	Internal Restricted	• To be treated as Highly Sensitive if includes any Highly Sensitive data
Official and unofficial transcripts	Internal Restricted	
Student or Employee ID Numbers	Internal Non-Restricted	
Other student record information (not designated as "directory information")	Internal Restricted	
Personnel files	Internal Restricted	• To be treated as Highly Sensitive if includes any Highly Sensitive data
Other personal human resource information	Internal Non-Restricted	• To be treated as Highly Sensitive, Sensitive or Internal Restricted if includes any of these types of data

Aggregations of names and/or contact information of DePaul applicants, students, faculty and/or staff	Students—Internal Restricted Faculty—Internal Non-Restricted Staff—Internal Non-Restricted	
Sensitive competitive data	Internal Restricted	• To be treated as Highly Sensitive if includes any Highly Sensitive data
Public safety incident reports	Internal Restricted	To be treated as Highly Sensitive if includes any Highly Sensitive data
Lists of hazardous materials stored at DePaul	Internal Restricted	
Insurance policy numbers	Internal Restricted	
Legal files	Internal Restricted	• To be treated as Highly Sensitive if includes any Highly Sensitive data
Other information reasonable people would conclude is private in nature	Internal Restricted	• To be treated as Highly Sensitive or Internal Restricted if includes any Highly Sensitive or Internal Restricted data