University of Portland

DATA RISK CLASSIFICATION GUIDELINES

1. **PURPOSE:** The intention of these guidelines is to define how the university classifies data risk and the systems that house that data. The guidelines are intended to augment the University's Information Security Policy, providing more specific protocols for data stewards, system administrators, application owners and end users, including faculty, staff and student employees. These guidelines are intended to protect the privacy and confidentiality of University data and prevent unauthorized access.

2. **SCOPE:** These guidelines define levels of risk for University of Portland data sets, servers and applications. Examples of each classification type and risk level are provided. A table of approved University services and the allowed data risk level for each is also included.

3. **GUIDANCE:** University of Portland has classified its information assets into risk-based categories for determining who can access the information and what security precautions must be taken to protect it against unauthorized access. As of January 2019, a new set of classifications has been established and is now in effect for University of Portland data and systems: **Level 1 - High Risk, Level 2 - Moderate Risk**, and **Level 3 - Low Risk**.

   a. **Level 1 - High Risk:** Data and systems are classified as High Risk if:
      - Protection of the data is required by law/regulation,
      - UP is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or
      - The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

   b. **Level 2 - Moderate Risk:** Data and systems are classified as Moderate Risk if they are not considered to be High Risk, and:
      - The data is not generally available to the public, or
      - The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or reputation.

   c. **Level 3 - Low Risk:** Data and systems are classified as Low Risk if they are not considered to be Moderate or High Risk, and:
      - The data is intended for public disclosure, or
      - The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.

   Special note to University of Portland researchers: Except for regulated data such as Protected Health Information (PHI), Social Security Numbers (SSNs), and financial account numbers, research data and systems predominately fall into the Low Risk classification. Review the classification definitions and examples below to determine the appropriate risk level to apply.

4. **DATA RISK CLASSIFICATION EXAMPLES:** Use the examples below to determine which risk classification is appropriate for a particular type of data. When mixed data falls into multiple risk categories, use the highest risk classification across all.

   a. **Level 1 - High Risk – Protected/Confidential**

- Passwords or credentials that grant access to level 1 and level 2 data
- PINs (Personal Identification Numbers)
- Birth date combined with last four digits of SSN and name
- Credit card numbers with cardholder name
- Tax ID with name
- Driver's license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name
- Social Security number and name
- Health insurance information
- Medical records related to an individual
- Psychological Counseling records related to an individual
- Bank account or debit card information in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Biometric information
- Electronic or digitized signatures
- Private key (digital certificate)
- Law enforcement personnel records
- Criminal background check results
- Donor contact information and non-public gift information

b. <u>Level 2 - Moderate Risk - Internal</u>

- Unpublished research data (at data owner's discretion)
- Student records and admission applications
- Non-public UP policies and policy manuals
- Non-public contracts
- UP internal memos and email, non-public reports, budgets, plans, financial info
- University and employee ID numbers
- Engineering, design, and operational information regarding UP infrastructure.
- Identity Validation Keys (name with)
    - Birth date (full: mm-dd-yy)
    - Birth date (partial: mm-dd only)
- Photo (taken for identification purposes)
- Student Information-Educational Records not defined as "directory" information, typically:
    - Grades
    - Courses taken
    - Schedule
    - Test Scores
    - Advising records
    - Educational services received
    - Disciplinary actions
    - Student photo
- Library circulation information.
- Trade secrets or intellectual property such as research activities
- Location of critical or protected assets
- Licensed software
- Vulnerability/security information related to a campus or system
- Campus attorney-client communications
- Employee Information
    - Employee net salary
    - Home address
    - Personal telephone numbers

- Personal email address
- Payment History
- Employee evaluations
- Pre-employment background investigations
- Mother's maiden name
- Race and ethnicity
- Parents' and other family members' names
- Birthplace (City, State, Country)
- Gender
- Marital Status
- Physical description
- Other

c. Level 3 - Low Risk - Public

- Research data (at data owner's discretion)
- Information authorized to be available on or through UP's website without network authentication. See the Registrar's guidance on Directory Information published on the up.edu website for details on what data is publicly available.
- Policy and procedure manuals designated by the owner as public
- Job postings
- University contact information not designated by the individual as "private"
- Information in the public domain
- Publicly available campus maps

5. **SERVER RISK CLASSIFICATION EXAMPLES:** A server is defined as a host that provides a network accessible service. View Minimum Security Standards: Servers.

a. Level 1 - High Risk

- Servers handling High Risk Data
- Servers managing access to High Risk systems
- University IT and departmental email systems
- Core campus infrastructure

b. Level 2 - Moderate Risk

- Servers handling Moderate Risk Data
- Database of non-public University contracts
- File server containing non-public procedures/documentation
- Server storing student records

c. Level 3 - Low Risk

- Servers used for research computing purposes without involving Moderate or High Risk Data
- File server used to store published public data
- Database server containing network IDs only

6. **APPLICATION RISK CLASSIFICATION EXAMPLES:** An application is defined as software running on a server that is network accessible. View Minimum Security Standards: Applications.

a. Level 1 - High Risk

- Applications handling High Risk Data
- Human Resources application that stores employee SSNs

- Application that stores campus network node information
- Application collecting personal information of donor, alumnus, or other individual
- Application that processes credit card payments

b. Level 2 - Moderate Risk

- Applications handling Moderate Risk Data
- Human Resources application that stores salary information
- Directory containing phone numbers, email addresses, and titles
- University application that distributes information in the event of a campus emergency
- Online application for student admissions

c. Level 3 - Low Risk

- Applications handling Low Risk Data
- Online maps
- University online catalog displaying academic course descriptions
- Bus schedules

7. **ACCEPTABLE USE AND STORAGE OF DATA:** University employees should always follow the guidelines and standards stated in the Technology Use Policy and Information Security Plan to keep their devices and connections secure and private. University data should not be stored or transferred on services or systems not managed or approved by the Univeristy: it should not be saved locally on a personally owned computer, stored on a third party online storage service like Google Drive, and it should not be posted or shared in any way on social media sites.

   Low and Medium Risk data can be used, stored, and transmitted for institutional purposes on standard University-managed services, such as Microsoft 365, up.edu email accounts, Teams, OneDrive, universiity shared network drives, and used through enterprise applications including Banner, Argos, PeopleAdmin, Moodle, etc.

   High Risk data should only be used and stored on applications properly configured to protect the information adequately. Where possible, it should remain in the secure enterprise applications such as Banner, PeopleAdmin, Raiser's Edge NXT, Moodle, and SoftDocs. Connecting to any such systems and accessing high risk data from off campus must be through a secure and encrypted channel such as the VPN (Virtual Private Network) connection managed by UP. High risk data should not be saved locally and only may be emailed by using encrypted email protocols (for UP users using Office 365, adding **[encrypt]** to the subject line (with the brackets) will encrypt the message.

8. **DATA INTEGRATIONS**: UP data of any classification will only be integrated into a third party application or service following a review and assessment by Information Services of the security pracitces and standards of the third party, and only after approval by the appropriate data owner for the type of data being shared (e.g. the Chief Financial Officer for budget and financial information and so on). Data integrations must use secure encrypted connections, such as sftp or VPN-protected connections regardless of the risk classification of the data.

9. **GENERAL INFORMATION/INQUIRIES:** Contact the UP help desk (help@up.edu) with any question about this policy or for a consultation to help find an appropriate and secure way to solve your data needs.