

# Data Classification Levels

All Seattle Pacific University [Institutional Data](#) is classified into one of the four classifications or sensitivity levels described below: **Restricted**, **Confidential**, **Internal**, and **Public**.

For more detail regarding handling of [Regulated Data](#), the [Regulated Data Chart](#) provides an overview of the types of regulated data that are permitted in various systems/platforms.

## RESTRICTED

Data are classified as *restricted* if:

- disclosure could cause severe harm to individuals and/or the university, including exposure to criminal and civil liability
- the University is required to self-report to the government or the public notice if the data is inappropriately accessed or handled
- legal and/or compliance regime may require assessment or certification by an external, third party
- loss of confidentiality, integrity or availability of the data has a significant risk to the University's reputation, finances, life and safety of the community, or increases security risk of other systems and data

*Examples include, but are not limited to:*

- [HIPAA](#) protected health records
- [PCI-DSS](#) regulated credit card information
- [FISMA](#) protected research
- Usernames and passwords

## CONFIDENTIAL

Data are classified as *confidential* if:

- disclosure could cause significant harm to individuals and/or the university, including exposure to criminal and civil liability
- the data is subject to legal and regulatory requirements due to data that are individually identifiable, highly sensitive and/or confidential
- loss of confidentiality, integrity or availability of the data has a moderate risk to the University's mission, reputation and/or finances
- exposure poses low risk to life and safety

*Examples include, but are not limited to:*

- Attorney client privilege records
- Financial accounts and direct deposit information
- Human Subject research data
- Social Security Numbers
- Student loan application information (GLBA)
- Passport, visa, and alien registration numbers
- Taxpayer and employer identification numbers
- Health insurance identification numbers

## INTERNAL

Data are classified as *internal* if:

- Disclosure could cause limited harm to individuals and/or the university with some risk of civil liability.
- May be subject to contractual agreements or regulatory compliance, or is individually identifiable, confidential, and/or proprietary.
- loss of confidentiality, integrity or availability of the data has a little risk to the University's mission, reputation and/or finances
- exposure poses no risk to life and safety

*Examples include, but are not limited to:*

- Student education records (FERPA)
- Student ID Number
- Research data or results prior to publication or the filing of a patent application
- Building plans, real-estate transactions, and associated information
- Threat assessments and preparedness strategies
- Contracts with third-party entities
- Donor records (individual)
- Employee records (multiple types)
- Emergency planning information
- Immigration documents (such as visas)
- Intellectual or other proprietary property
- University non-public financial information

## PUBLIC

Data are classified as *public* if:

- data is intended for public release
- loss of confidentiality, integrity or availability of the data has a no risk to the University's mission, reputation and/or finances
- exposure poses no risk to life and safety

*Examples include, but are not limited to:*

- Course catalogs and time schedule
- Faculty, staff, and student directory information (unless there is a privacy block)
- General institutional and business information not classified as **Restricted, Confidential, or Internal**
- Information in the public domain
- Public websites
- Published research (barring other publication restrictions)
- Research Awards
- Research Proposals