Data Classification and Protection Levels: Impact of disclosure or compromise

**P4 - High**
Summary Definition: Information and IT Resources requiring the highest level of confidentiality or integrity, including Notice-Triggering data and “Shared-Fate” data and systems.

Key examples:
- “Notice-triggering” data elements such as SSN, driver’s license, financial account, or credit card numbers, personal medical or personal health insurance information
- Passwords, PINs and passphrases
- Financial aid and student loan information
- Individually identifiable human subject research data or genetic information

**P3 - Moderate**
Summary Definition: Information and IT Resources whose unauthorized use, access, disclosure, modification, loss or deletion could result in moderate harm or damage.

Key examples:
- Personally identifiable information not already classified as P4
- FERPA-Protected Student Records (including Student ID) not containing P4 information
- Staff and academic Personnel Records (including Employee ID) not containing P4 information

**P2 - Low**
Summary Definition: Institutional Information and IT Resources that are generally not intended for public use or access and may only be accessed on a need-to-know basis.

Key examples:
- Information intended for release only on a need-to-know basis
- De-identified human subject or patient information (with negligible re-identification risk)
- Public Directory Information for faculty, staff, and students who have not requested a FERPA block

**P1 - Minimal**
Summary Definition: Information intended for public access, but whose integrity is important.

Key examples:
- Public-facing informational websites
- Course listings and prerequisites
- Press releases
- Published research

For full definitions and additional examples refer to UC Berkeley’s Data Classification Standard: https://security.berkeley.edu/data-classification-standard