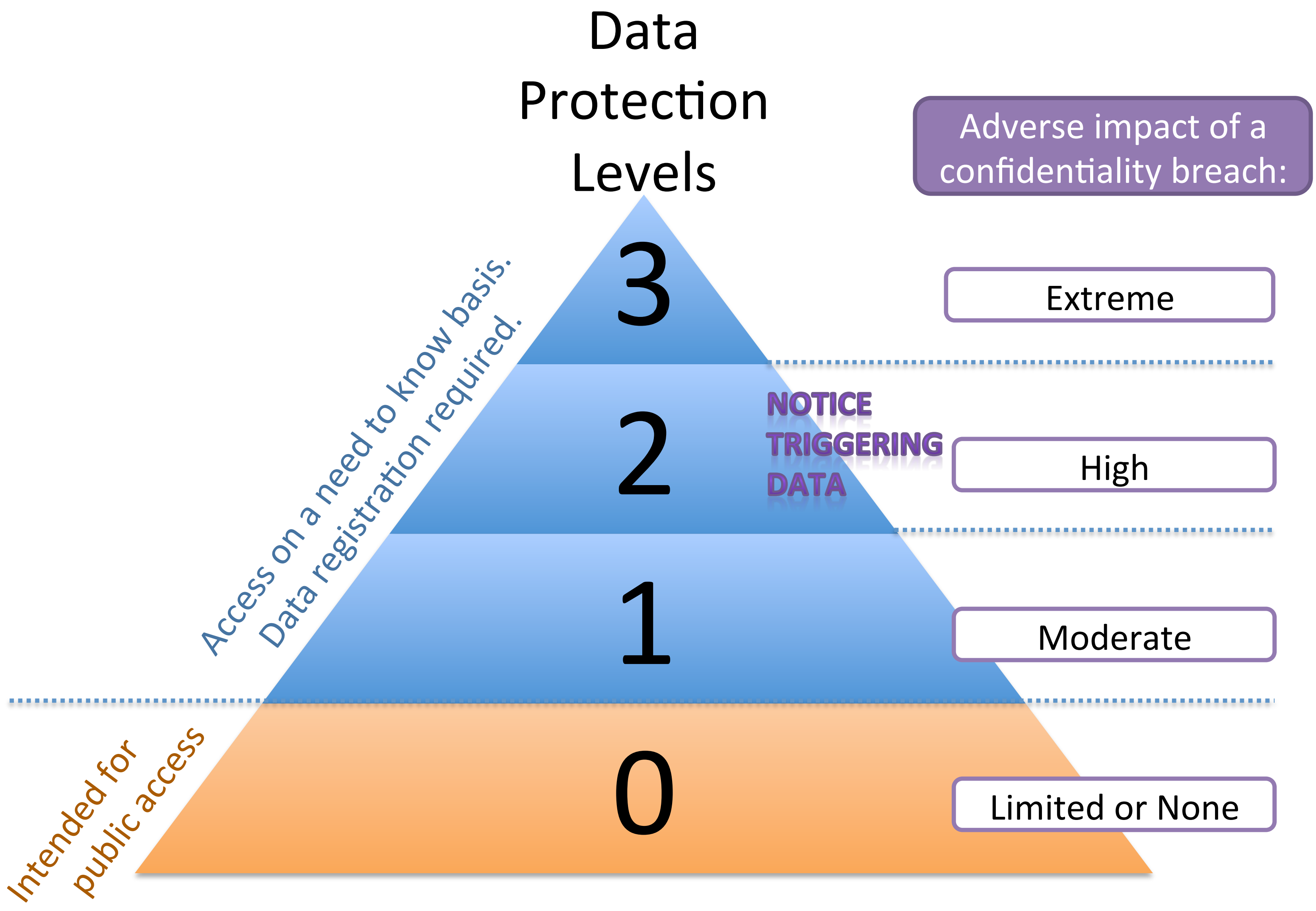
Data Classification Standard


Data Protection Levels
Adverse impact of a confidentiality breach:
3
Extreme
2
NOTICE TRIGGERING DATA
High
1
Moderate
0
Limited or None
Access on a need to know basis.
Data registration required.
Intended for public access

Data Classification Standard

http://security.berkeley.edu/data-classification

Data Protection Level	Adverse impact*	Sample Data Types (not an exhaustive list)
Level 3	Extreme	Data that creates extensive "shared-fate" risk between multiple sensitive systems, e.g., enterprise credential stores, backup data systems, and central system management consoles.
Level 2	High	Data elements with a statutory requirement for notification to affected parties in case of a confidentiality breach: • **Social security number** • **Driver's license number, California identification number** • **Financial account numbers, credit or debit card numbers; financial account security codes, access codes, or passwords** • **Personal medical information** • **Personal health insurance information**
Level 1	Moderate	Information intended for **release only on a need-to-know basis**, incl.: Personal information not otherwise classified as Level 0, 2 or 3, and Data protected or restricted by contract, grant, or other agreement terms and conditions, e.g.,: • FERPA student records (including Student ID) • Staff and academic personnel records (including Employee ID) • Licensed software/software license keys • Library paid subscription electronic resources
Level 0	Limited or None	Information **intended for public access**, e.g.,: Public websites, Course listings and pre-requisites, and Public directory data: **Staff:** Name, Date of hire, Current position title, Current salary, Organizational unit assignment, Date of separation, Office address, Office telephone number, Current job description, Full-time or part-time, and Appointment type **Students (unless the student has requested that information about them not be released as public information):** Name, Address, Telephone, Email, Dates of attendance, Number of course units in which enrolled, Class level, Major field of study, Last school attended, Degrees and honors received, Participation in official student activities, Weight/height (intercollegiate athletic team members only)

Public records requests, litigation or other legal obligations may require disclosure of information in any data class.

* Considerations for evaluating potential **adverse business impact to the campus** due to loss of data confidentially or integrity:

- Loss of critical campus operations
- Negative financial impact (money lost, opportunity cost, data valuation)
- Damage to the reputation of the campus
- Potential for regulatory or legal action
- Requirement for corrective actions or repairs
- University or campus mission, policy, or principles

Office of the CIO – April 5, 2013