Protection Level – Classification Guide

Supplemental Guidance

1. **Institutional Information** - A term that broadly describes all data and information created, received and/or collected by UC.
   
   a. Example 1: Information contained in a database, such as employee personnel records or records pertaining to student enrollment and grades, is Institutional Information.
   
   b. Example 2: Activity log data from a server application or network device is Institutional Information.
   
   c. Example 3: Emails sent and received pertaining to UC business are considered Institutional Information.
   
   d. Example 4: Instrument measurements from academic research, collected manually or electronically, are Institutional Information. Example 5: Electrical use data collected by a building automation system is Institutional Information.

2. **IT Resource** - A term that broadly describes IT infrastructure, software and/or hardware with computing and networking capability. These include, but are not limited to: portable computing devices and systems, mobile phones, printers, network devices, industrial control systems (SCADA, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic media, Logical Media, biometric and access tokens and other devices that connect to any UC network. This includes both UC-owned and personally owned devices while they store Institutional Information, are connected to UC systems, are connected to UC Networks, or are used for UC business.

3. **Contact OIT Security** - For additional guidance please reach out to securityreviews@uci.edu or visit the OIT Security Team Webpage.

4. **Impact to Privacy** – It is important for Units to understand what Institutional Information they have and how the unauthorized disclosure of that information could impact an individual’s privacy. Privacy at UCI consists of: (1) the individual’s ability to conduct activities without concern of or actual observation and (2) the appropriate protection, use, and release of information about individuals.

Some things to think about include:

   a. Can the elements of the information collected be used for:
      
      i. Discrimination
      
      ii. Surveillance
      
      iii. Blackmail or humiliation
iv. To hurt an individual or put them in severe harm or danger

b. Authorized use and access of data
   i. What did individuals expect the Campus to do with the information (authorized uses)?
   ii. Who is allowed to receive this information (authorized disclosures)?
   iii. Did we tell individuals how we would use, store, share, and delete the information? (notice of privacy practices)
   iv. How do we safeguard the data to prevent unauthorized access, use, or disclosure?

Please visit the UCI Privacy Webpage for more details.

5. Large Data Set Amount – The Unit best understands their Institutional Information and the risk associated with it. The definition of “large” could be different for every Unit. It’s important to think about if this information was ever compromised how much of an impact would it have to the Campus. The definition of “Large” should be based on the risk associated with the type of data involved. Below are some general guidance examples of “large” vs “small” data sets:

   a. Large Data Sets
      i. Extract of employee data of all UCI employees, or of large units or large workgroups.
      ii. Extract of student data of all UCI students, or of large schools or large academic programs.

   b. Small Data Set
      i. Extract of employee data in an individual unit.
      ii. Extract of student information of students enrolled in a school or small academic program.

6. Context and Comprehensive – It is important for Units to understand what Institutional Information and IT Resources they have and the context on how it is being used or how it can be used. Think about if anyone can misuse or abuse the information in a malicious way. Below are some general guidance examples of what someone can use the data elements to do:

   a. Steal an individual’s identity or impersonate someone
   b. Reset an individual’s login credentials
   c. Change someone’s account information or status
   d. Etc.
7. **Special Security Requirements** – Special security requirements can be special controls required from an external party. These requirements can be tied to federal grants, research funding, insurance agreements, and other contract or obligations. The requirements of the controls will help determine the appropriate protection level.