UNIVERSITY COMPLIANCE
Youth Protection

Office of Youth Protection: Information Security Guidelines

Information related to non-enrolled minors participating in activities, events, or programs offered by the University of Arizona or held on University Property must be classified and handled per applicable Information Security Polices and comply with guidelines established by the Information Security Office and the Office of Youth Protection. This expectation applies to the wide variety of information a program may generate, collect, process, disseminate, and dispose of.

Program Supervisors are responsible for the administration, coordination, management, and operation of (a) program(s) registered with the Office of Youth Protection. Program Supervisors responsibility includes understanding and/or establishing the controls for program-related University Information (in any format including both paper and electronic formats) including its generation, collection, processing, dissemination, and disposal. Program Supervisors responsibility also includes applying appropriate controls when storing, processing, and transmitting University Information.

While each program is responsible for adhering to existing Information Security policies, standards, and guidelines, which necessitate contextual evaluations of program-related University Information, the Office of Youth Protection (OYP) establishes these minimum expectations:

- Program-related University Information should generally be classified as non-Public (i.e. Restricted), as the risk of public disclosure of information relating to non-enrolled minors poses greater than little risk to the University or University-Related Persons and/or those that are encumbered by regulatory, statutory, or contractual obligations for confidentiality.
    - If a Program Supervisor determines that program-related University Information is less sensitive than the Office of Youth Protection expects they must contact the OYP for consultation.
- The Office of Youth Protection does not expect that a program would generate, collect, process, or store University Information that would fall under the oversight of a designated Compliance Office (e.g. HIPAA, ADA, FERPA).

- If a program determines that they generate, collect, process, or store University Information, that would fall under the oversight of a designated Compliance Office they must contact the appropriate office for consultation.

Resources:

Information Classification and Determination Policy, ISO-400

Information Resource Classification Standard, ISO-400-S1

Information Resource Classification Guideline, ISO-400-G1

Information Handling Standard, ISO-400-S2

Information Handling Guideline, ISO-400-G2