# Information Security Strategic Plan

# Strategic Plan

Ensure appropriate security for university information and IT systems, while promoting security awareness among the administration, faculty, staff, and students.

# Strategic Directions

- Review, update, and develop policies, standards, procedures and best practice guidelines to ensure a safe, compliant, and properly risk managed computing and network environment. In collaboration with all appropriate University representatives the Chief Information Office (CIO) will lead efforts to develop and launch a suite of information security policies, standards and guidelines, based on the ISO/IEC 27002 code of best practices for information security. These policies, standards, and procedures will formally establish UAM's Information Security Program.
- Ensure that all employees are aware of their information security responsibilities
    - Train employees about the role they play in protecting the University's information assets.
    - Broaden the information security knowledge of campus technical personnel to improve the university's overall security effectiveness
- Develop a campus-wide information security risk management program to evaluate threats and vulnerabilities and assure creation of appropriate remediation plans.
    - Increase the quality of the decision processes associated with the protection of the University's information assets.
    - Evaluate information security controls and countermeasures to mitigate risks to an acceptable level on a set time period
    - Develop a set of security of assessment services that can be offered to schools or departments
    - Protect our students and employees from potential crimes such as identity threat.
- Standardize the University's information security incident response and reporting.
    - Establish campus-wide security incident response processes
    - Develop communications plan
    - Develop an awareness plan
    - Develop monitoring and review plan