Information Security Policy

Information Security Department

PURPOSE:

This policy establishes Chapman University's strategy and responsibility for ensuring all data, network, and computing information assets will be available to the community, be protected commensurate with their value, and are administered in conformance with federal and state law. Reasonable measures shall be taken for protecting these assets against accidental or unauthorized access, disclosure, modification or destruction, as well as to reasonably assure the confidentiality, integrity, and availability of the information assets are controlled by the University.

SCOPE:

Information assets addressed by this policy include all data, information systems, computers, network devices, as well as documents and verbally communicated information.

POLICY:

Chapman University requires members of its faculty, staff, student body, and any 3rd party vendors of network or computing services to fulfill the individual and institutional standards of this Information Security policy.

The goal of this policy is to:

- Establish a University-wide information security framework to appropriately secure access to information resources and services;
- Establish safeguards to protect against unauthorized access to, use, or sharing of, *sensitive information* that could potentially result in harm to the University or to members of the University community;
- Protect against anticipated threats or hazards to the security of information assets;
- Comply with federal, state, and local law, University policies, and agreements binding the University that require the University to implement applicable *security safeguards*.
- Have individual and shared responsibilities to protect the information assets controlled by the University in accordance with federal, state, and local law, University policies, and agreements binding the University.
- Identify and track sensitive and critical *Information assets* under its control. *Information assets* will be classified relative to the level of risk that their compromise may pose to the institution. *Information asset* classification standards and guidelines will be adhered to.
- Periodically conduct risk assessments around its sensitive and critical *information assets*. Risk assessments will prioritize risks and recommend appropriate mitigation strategies.
- Report and manage information security incidents in accordance with established policies and guidelines.

- Implement *Security safeguards* that are appropriate to *information asset sensitivity*, *criticality*, and the level of risk identified in the risk assessment process.

Additional information that supports this policy can be found in the Information Security Policy Standards.

ADMINISTRATION:

The Director of Information Security responsibilities include:

a) Develop, maintain, and implement an information security plan. The plan will identify applicable regulations and will define unit security initiatives.

b) Communicating this policy and standards to the community and ensuring appropriate education and training;

c) Implement and test safeguards; ensure safeguards are implemented, tested, and maintained

d) Designating individuals for information security roles which address network and computing assets, ensuring they are properly trained, and ensuring their ongoing participation in University-wide information security activities;

e) Ensuring the implementation of information security plans by the Director of Information Security;

f) Ensuring departmental collaboration university wide on the implementation of the Information Security Program.

The Director of Information Security is responsible for:

a) Directing and coordinating the Information Security Program; effectiveness assessments conducted by Internal Audit and Department of Information Security

b) Determining unit-level compliance with this policy;

c) Providing a focal point for oversight of handling information security incidents as;

d) Establishing security metrics, tracking the progress of the Information Security Program, and providing a University-wide risk profile;

e) Assisting departments in fulfilling their information security requirements.