Standards listed below. All University units must meet the minimum applicable requirements established in each Information Security Standard for the protection of University IT Resources. Individual units may adopt additional Information Security Standards that exceed these minimum requirements. After careful review, the CIO may grant a written exemption to a particular Information Security Standard when doing so serves the best interests of the University. Other Information Security requirements are outlined in the Information Security-related University Policies cross-referenced with this policy below. The University's Information Security Standards include the following:

Auditing, Logging, and Monitoring

Data Backup and Disaster Recovery

Enterprise System Change Management

Information Technology Risk Assessment

Secure Data Center Physical Security

Software Patch Management

Vulnerability Management and Scanning

F. Training and Implementation

This policy governs all data and IT Resources owned by or under the University's control. It applies to all campuses, units, and University Community Members wherever located. The CIO, Director of Information Security Services, and the Information Security Committee are required to establish and revise the standards, policies, and controls identified herein. All units and University Community Members must adopt and follow the controls and policies set forth herein. Each of the University's senior executives is responsible for implementing Information Security Standards and all other applicable requirements within their respective areas of jurisdiction, and for providing all training that may be necessary or prudent.

G. Standard Information Security Contract Language

Information Security Services provides standard language