**Annual and Scheduled activities/requirements/reviews**

1. Review of confidentiality agreements currently in place
2. Review of user access to L1 and L2 applications, and administrative access to systems
3. Risk Assessment of assets containing L1 data at least every 2 years
4. Segregation of Duties Procedures and Reporting – annual/monthly/quarterly reviews certification
5. PCI Compliance
6. Annual review of information security plan/program
7. Annual Review and certification of Record Retention
8. Annual review of all system (if part of a system) and University’s policies, standards, guidelines
9. Annual review of the University’s Information Security governance structure
10. Annual review of University Incident Response Plan

**Required Procedures/Standards/Guidelines/Practices**

1. Information Security Program which must include sections on:
   1. Roles and responsibilities within the program
      1. Document the organizational structure for the university information security program
      2. Document ISO appointed by University President/Chancellor and/or AVC for ITS
   2. Provide for Confidentiality, Integrity and Availability (CIA) of information (paper or electronic)
   3. Include Risk Management program
      1. Identify risk
      2. Monitor risk
      3. Develop plan to mitigate/transfer or accept risk
      4. Develop process to identify assess and monitor assets containing L1/L2 data
      5. Document frequency, methodology and migration strategies of assessments
      6. Develop and document method of tracking risk assessments and decisions
   4. Incident Response program
      1. Define and categorize incidents
      2. Designate CIRT/CSIRT
      3. Procedures for documenting, notification, remediation and reporting
      4. Lessons learned
      5. Corrective actions and mitigations
   5. Security Training and Awareness plan
   6. Comply with applicable Laws, Regulations and University Policies
   7. Standards for Access Control
      1. Need to know and least privilege
      2. Segregation (or Separation) of Duties
      3. Access Review
      4. Access Modification
   8. Procedures to revoke (physical and logical) access promptly when appropriate
   9. Campuses must have procedures to identify critical information systems and protected data that is stored or transmitted on campus systems
   10. Implement controls to secure L1 data on mobile devices
   11. Implement controls for monitoring systems to detect malicious behavior
2. Procedures for background checks for positions that involve access to L1 information assets
3. Develop, implement and document configuration standards
4. Change Management procedures that include additional reviews when significant changes to L1 or L2 information assets are in scope
5. Develop and Maintain inventory of information assets containing L1 or L2 data
   1. Designated Data Owners
   2. Defined Security Requirements
   3. Manage Information Assets

**Training and Awareness**

1. New Hire Orientation
2. On Line Training
3. Awareness Campaigns
4. Financial Aid Office
5. Testing Office
6. FERPA
7. PCI
8. HIPPA

**Additional Responsibilities**

1. Protection of Physical Areas that require protection because they store sensitive data (data centers and network utility closets)
2. Support Business Continuity and DR
3. Policy Compliance
   1. Procedures that ensure investigations of students and employees are in compliance with laws, regulations, collective bargaining agreements (if a union shop) and University Policy
4. Red Flag Rules Compliance