Information Management and Classification Process

Identification - Identify all information assets

a. Data Gathering
    i. Surveys
    ii. Questionnaires
    iii. Group Meetings
    iv. Personal interviews
b. Resources – Solicit information 'from' or assign process 'to'
    i. Department Managers/Deans
    ii. University Staff/Users
    iii. Departmental IT (Tier I)
    iv. IT Developers/Administrators

2. Documentation - Document assets within the inventory listing
    a. Information asset title
    b. Location of asset (data)
        i. Server
        ii. Directory
        iii. Database
        iv. File Cabinet
    c. Data Owner
    d. Data Custodian
    e. Type of asset
        i. File
        ii. Application
        iii. Website
        iv. Hardcopy
    f. Current safeguards (encryption, data center, locked cabinet, etc.)
3. Classification –Classify assets within the inventory listing
    a. Confidentiality
        i. Confidential
        ii. Proprietary – Internal Use Only
        iii. Public
    b. Integrity
        i. High
        ii. Medium
        iii. Low
    c. Availability
        i. 24x7 ii. 12x6
        iii. Best Effort
        iv. DR-recovered tape
        v. DR-recovered redundancy (high availability)

4. Control - Develop guidelines based upon classifications
    a. Confidentiality
        i. Labeling
        ii. Handling/Transmission
        iii. Storage
        iv. Disposal
    b. Integrity
        i. Access Controls
            1. Authentication/Log In/Multi-Factor
            2. Role Based Access (RBAC)
            3. Periodic Access Reviews
            4. Segregation of Duties
            5. Non-Disclosure/BAA 3rd Party Contracts ii. Approval Process (Authorization)
        iii. Encryption
        iv. Monitoring/Audit and Logging
        v. Network Isolation
        vi. Infrastructure/IDS/Anti-Virus/Patch Mgt./Vulnerability
        vii. Vulnerability Scanning/Penetration Testing
        viii. File Integrity Checking
        ix. Change Management, Secure Coding, Input Validation, SDLC c. Availability
        i. Backup, Off-site storage
        ii. High Availability (Redundancy) or Tape Recovery
        iii. Custodian Service Level Agreements
        iv. Support Personnel Cross Training
        v. Business Continuity/DR Planning and Testing
5. Compliance - Implement Triggers for review and modification
    a. Annually as a default
    b. Employee Life Cycle (new user, transfer, term)
    c. Change Management Process (system/application modification)
    d. SDLC – System Development Process (new system/application)