Technical Standard for IT Enterprise System Classification, Risk Management and Disaster Recovery

PURPOSE

This technical standard defines the College's requirements for:

- inventorying, classifying and documenting supported IT systems and applications;
- the requirements for documenting Risk Assessment Plans and Disaster Recovery Plans for internally hosted systems;
- the requirements for vendors that host sensitive or critical systems.

STANDARD

Maintenance of an accurate *Enterprise Systems Inventory* is the responsibility of IT Services.

Documentation for each inventoried application includes:

- Highly Sensitive Data Indicator
- System Restoration Priority Tier
- Externally Hosted System Indicator

Systems Storing Highly Sensitive Data

Any enterprise system storing highly sensitive data, as defined in the college's Data Classification Standard within the *Administrative Data Management and Access Policy,* must be flagged as such.

All internally hosted enterprise systems containing highly sensitive data should have a documented Risk Assessment plan, with a formal risk assessment completed annually.

All externally hosted enterprise systems containing highly sensitive data should include additional vendor contractual terms and conditions, including a requirement for annual copies of vendor SSAE-16 audit compliance reports.

Systems With Critical Availability Requirements

Enterprise systems are categorized in terms of high availability requirements, or restoration priority order.

Each enterprise system listed in the *Enterprise Systems Inventory* will be classified per restoration priority, as follows:

- Tier 1 - Highest availability and highest restoration priority requirement; recovery begins immediately upon identification of issue, including after hours.
- Tier 2 - Medium restoration priority; to be restored after recovering all applicable Tier 1 systems. If problem is identified after working hours, recovery begins at 7:30 am the following business day, or at 9:00 am on Saturday/Sunday.
- Tier 3 - lowest priority; to be restored after recovering all applicable Tier 2 systems. If problem is identified after working hours, recovery begins at 8:00 am on the next business day (Monday through Friday).

All internally hosted systems classified with a Tier 1 restoration priority will have a documented Disaster Recovery plan in place; DR Plans should be reviewed and updated annually, including verification of annual disaster recovery testing activities.

All externally hosted Tier 1 systems should have special vendor contractual terms and conditions regarding system availability and disaster recovery.

RELATED INFORMATION

Enterprise Systems Inventory

APPROVALS AND REVISIONS

Approved by Chief Technology Officer, May 21, 2012

Revision History:

10/8/12 - Revised to include more specific restoration/recovery "Tier" definitions