Security Standard: Solutions Life Cycle Management

Scope

The standard applies to new IT services (including third-party and RIT-hosted, and software as a service) that meet any one or more of the following:

- host or provide access to Private or Confidential information
- support a Critical Business Process

Requirements

The following security controls are required to be implemented.

1. **Engagement**
   1.1. Contact the Information Security Office and ITS prior to investigating, evaluating, selecting, or developing a new solution.

2. **Planning and Preliminary Risk Assessment**
   2.1. ITS will determine applicable security requirements and provide a preliminary risk assessment.

3. **Business Contract Phase**
   3.1. Any proposed contract will be reviewed and revised in accordance with procurement services procedures under the direction of RIT Procurement Services.

4. **Development**
   4.1. The solution owner will inform ITS of any changes to the security requirements during development.
   4.2. Solutions development, testing, and production should be performed in separate environments.
   4.3. Test data should not include Private or Confidential information unless the security controls in test and development are the same as those in production.
   4.4. The solution owner should identify solution administrators.

5. **Security Review**
   5.1. ITS will conduct a Security Review.
   5.2. ITS will perform an appropriate vulnerability assessment and penetration test before solution implementation.

6. **Maintenance**
   6.1. The solution owner is responsible for ensuring that the security impact of any change is evaluated and notify ITS and the Information Security Office accordingly if there is a potential increase in risk.

7. Solutions Retirement/Disposal

7.1. The solution owner will ensure that the solution is evaluated at an appropriate interval and retired if appropriate.

7.2. The solution administrator should ensure that Information is retained in accordance with the Records Management Policy, and to accommodate future technology changes that may render the retrieval method obsolete.

7.3. The solution administrator should ensure that Information is disposed of as required by the Information Access and Protection Standard.

Effective Date: January 23, 2015

Standard History:
November 11, 2013
October 19, 2015

Summary of Changes—Solutions Life Cycle Management Standard, 10/19/2015

We've made changes to the standard to incorporate the move of certain operational responsibilities from the ISO to ITS.

Section 1 changes

- Contact the ISO AND ITS (previously just the ISO)

Section 2 changes

- ITS, not the ISO, will determine applicable security requirements and provide a preliminary risk assessment

Section 3 changes

- Removed web link to procurement services procedures

Section 4 changes

- Solution owner to inform ITS, not the ISO, of changes to security requirements during development.

Section 5 changes

- ITS, not the ISO, will conduct security review and perform appropriate vulnerability assessment and pen test

Section 6 changes

- Solution owner to notify ISO AND ITS of any increase in risk from changes after deployment