ITS Configuration Management Policy

<table>
<thead>
<tr>
<th>Author</th>
<th>AdamDodge, ITSecurityOfficer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Date</td>
<td>February 20, 2009</td>
</tr>
<tr>
<td>Status</td>
<td>InternalITS</td>
</tr>
<tr>
<td>DateEffective</td>
<td>September 8, 2009</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Public</td>
</tr>
<tr>
<td>Owner</td>
<td>InformationSecurity, ITS</td>
</tr>
<tr>
<td>Authorization</td>
<td>M.K.Chatterji, Asst.VPforITS</td>
</tr>
</tbody>
</table>

**Policy Statement**

All information resource owners and/or information resource operators must document the baseline configuration for any and all information resources for which they are responsible in order to document the purpose and intent of the resource as well as how the resource is currently configured. In addition to baseline configurations, all information resource owners must establish change management guidelines that detail the allowed method for implementing changes to a resource.

**Reason for Policy**

It is important to document information resource configuration and change management information for many different reasons. Such configuration and change information allows for easy knowledge transfer between individuals responsible for information resource operation. In addition, configuration and change documentation and procedures can help information resource owners ensure that the setup and continued maintenance of their resources are done according to approved standards. Documenting and reviewing baseline configurations as well as continued system changes allow the University to meet the changing demands of campus computer while ensuring that information resources are deployed using approved configurations that do not create unacceptable levels of risk to protected and/or private information.

**Entities Affected By This Policy**

Any individual, group or department that wishes to run any telecommunication equipment, computer systems, applications, network equipment, and other equipment, goods, and services related to the processing, storage, transmission and collection of University information.
**Contacts**

Questions about the policy in general should be directed to:

IT Security Officer  217-581-1942

Questions about the application of this policy on a specific information resource should be directed to the individual responsible for the resource

**Definitions**

*Information Resource* - Information Resources are defined as any items, including telecommunication equipment, computer systems, applications, network equipment, and other equipment, goods, and services related to the processing, storage, transmission and collection of University information.

*Information Resource Operator* – Information Resource Operators are defined as any individual responsible for the operation, maintenance, support and/or administrator of an information resource.

*Information Resource Owner* – Any individual, department or group responsible for the creation, storage, protection and/or dissemination of University information and information resources for which no other Owner exists. For example, faculty are considered the Owners over their course materials and students are considered the Owners over their own work. The term Owner does not imply ownership in any legal sense. Owner only identifies the individual with the primary responsibility for University information and/or an information resource.

*Non-Public Information* - Non-public information is any information designed for internal university use and not for release to the public. This information includes, but is not limited to, memos, internal e-mails, reports, course work, etc. This information may be subject to open records laws, however the intent of the work is not public use.

*Protected Information* – Protected information is any information that is currently covered by local, State or Federal regulation or contractual obligations such as PIPA, FERPA, HIPAA, GLBA, and PCI DSS.

**Responsibilities**

*Information Resource Operators*

Information Resource Operators are responsible for establishing baseline configurations for each systems, or utilizing approved baselines such as the Center for Internet Security benchmarks, as well as creating and maintaining all baseline configuration outlined in this policy.
Information Resource Operators are responsible for following change management procedures established by the Information Resource Owner.

*Information Resource Owners*

Information Resource Owners are responsible for establishing change management procedures including, but not limited to, what individuals may request and/or initial a resource change, allowable maintenance windows, change proposal reviews, and change implementation review.

Information Resource Owners are ultimately responsible for ensuring that all requested changes do not negatively impact the overall security of the system. This includes careful considerations of insecure services such as FTP or TELNET, regulatory requirements such as FERPA, HIPAA, PIPA, etc, the addition of external connections given the information already on the resources and all increased access requests.

*Information Security*

Information Security is responsible for working with information resource owners and operators to review baseline configurations of all information resources on campus. Reviews will be done to ensure that the levels of risk facing each resource is acceptable for the information resource owner and that there are not regulatory requirement issues with current baselines.

Information Security is responsible for the creation and designation of approved generic baselines to help information resource owners and operators quickly configure information resources in a manner already approved by the university.

**Principle**

*Baseline Configuration*

- All information resources owners and/or operators are responsible for establishing baselines configurations that follow industry recognized best practices
  - Information resource owners are strongly encourage to utilize the Center for Internet Security configuration benchmarks whenever possible
  - Information Security will work to develop “EIU approved” guidelines that meet the requirements of University policies and follow best practices
- Baseline configurations must include the following information
  - A description of the resource
  - The intended use of the resource
  - The types of information authorized by resource owner to be stored on the resource
o The logical placement of the resource in the existing infrastructure
o A list of resource components and component identifiers (ie S/N, Model Number, etc)
o The base operating system of the resource
o The additional software loaded on the resource
o The base operating system configuration
o The configurations of any additional software

- Generic baseline configurations may be created for each class of resource including, but not limited to, desktops, laptops, and servers
  o If using a generic baseline configuration, information resource owners and/or operators are responsible for documenting how configuration of the resource differs from that of the generic baseline
- Baseline configurations must be approved by Information Security prior to implementation on active resources containing protected and/or non-public university information
- Baseline configurations must be updated by information resource owners and/or operators whenever a change occurs

**Configuration Change Control**

- All information resource owners will establish configuration change control procedures for major changes including, but not limited to, software version upgrades, addition/removal of software/hardware/service, and configuration changes
- All configuration change control processes must include provisions for at least the following:
  o A change proposal, for supervisor approval, including the justification for the change, listing of all modifications/upgrades/changes to be made, implementation schedule, change test/evaluation plans and change review plans
- All configuration changes must be documented as part of the configuration change control processes and kept on file by the information resource operators
- Configuration change control documentation should be reviewed annually by Information Security for systems containing non-public and/or protected information

**Configuration Change Control Management**

- Configuration changes may only be altered by authorized individuals as defined by resource owners and/or operators
- Configuration documentation must accurately reflect resource configuration and remains up-to-date
- Planned configuration changes may not negatively impact information security or conflict with industry best practices

**Related Documents**
TBD

**Supporting Policies, Procedures and Guidelines**
ITS General Configuration Guidelines (TBD)
ITS System Maintenance Security Policy
Center for Internet Security Configuration Baselines

[PDF to Word]