C4 3.4: Configuration Management

Created by Purdue University NSF # 1840043

800-171 Rev. 1 Mapping	Control Family	Required Control	Implementation	Program/Policy/Procedure Reference	Control Gap
3.4.1	C4.3.4.1	Develop and maintain inventories of authorized hardware; inventory should be reviewed no less than annually or upon significant changes to the environment.	☐Implemented ☐Planned to be Implemented (see: Control Gaps) **Description:**	Per the Information Security & Privacy Policy (VII.B.8), each area of the University with IT Resources has an IT Security Officer assigned who aids in the identification and prioritization of Information Assets and IT Resources based on classification, criticality and business value . Purdue Security Contacts (PSCs) are required to maintain an inventory of network-connectable devices under their control according to guidelines established by the Coordinator of Incident Response (CIR) per the Incident Response Policy (VII.B.3).	
3.4.2	C4.3.4.2	In consultation with appropriate IT Security stakeholders, develop authorized security settings/configuration on baselines or utilize central templates.	☐Implemented ☐Planned to be Implemented (see: Control Gaps) **Description:**		
3.4.3	C4.3.4.3	Establish and document a change control process that includes review and approval of changes by IT and security staff as well as relevant stakeholders. Document changes and be prepared to	☐Implemented ☐Planned to be Implemented (see: Control Gaps) **Description:**		

		update the control descriptions in the system security plan at annual review.			
3.4.4	C4.3.4.4	Perform security impact analysis of applications, updates, and patches in consultation with IT staff and appropriate IT Security stakeholders where necessary. A separate test environment is recommended where appropriate. Patch-management general timeframes: Within seven days, review risk and prioritize reported critical and high risk (based on CVSS 2.0 or above scoring) vulnerabilities for remediation. Vulnerabilities not remediated within 30 days must be documented with mitigating controls and residual risk. Medium and low risk vulnerabilities must be risk assessed within 30 days.	☐Implemented ☐Planned to be Implemented (see: Control Gaps) **Description:**		
3.4.5	C4.3.4.5	Create and maintain a list of personnel authorized to make changes to the information system. Review/update the list at termination/transfer of personnel and no less than annually. Document review.	☐Implemented ☐Planned to be Implemented (see: Control Gaps) **Description:**		
3.4.6	C4.3.4.6	Disable all unnecessary processes. Only install required applications. Required applications are applications necessary for the storage/processing/transmission of restricted data in the furtherance of business purposes. Email clients or general web browsing are not essential applications on servers. Review frequency	☐Implemented ☐Planned to be Implemented (see: Control Gaps) **Description:**		

		should be based on risk but no less than annually.			
3.4.7	C4.3.4.7	**Reference Required Control C4 3.4.6**			
3.4.8	C4.3.4.8	**Reference Required Control C4 3.4.1**			
3.4.9	C4.3.4.9	Software acquisition and installation must follow a documented procedure.	☐Implemented ☐Planned to be Implemented (see: Control Gaps) **Description:**		