Audit Report - Copper Team

Conducted by :

Sarat Sreeram

Abdallah Daimi Syed

Kshitij Tapre

Vedant Vashistha

Eliel Zhuwankinyu

Executive Summary

Objective of the Audit :

The primary aim of this audit was to assess the alignment of Illinois Institute of Technology's IT policies with the NIST SP 800-171 standards. This standard provides a framework to safeguard Controlled Unclassified Information (CUI) in non-federal information systems and organizations, which is crucial for maintaining the confidentiality, integrity, and availability of sensitive data.
Scope of the Audit:
Our comprehensive audit covered five critical areas:

- Patch Management Policy
- Encryption Standard
- Configuration and Baseline Standard
- Configuration Management Plan
- System Services and Asset Lifecycle Management Plan

Each policy was meticulously reviewed to ensure that it not only complies with the NIST SP 800-171 requirements but also effectively supports the institution's needs for security and operational efficiency.

Importance of NIST SP 800-171 Compliance :

Adhering to NIST SP 800-171 is vital for several reasons:

- Enhancing Data Security: Compliance helps in strengthening the protection mechanisms around sensitive information, reducing the risk of data breaches.
- Building Trust: Aligning with recognized standards reassures stakeholders about the institution’s commitment to cybersecurity best practices.
- Regulatory Compliance: Meeting these standards is often a prerequisite for engaging in contracts with government bodies, thereby expanding opportunities for collaboration and funding.
- Proactive Risk Management: By complying with these guidelines, the institution can anticipate and mitigate potential security threats before they manifest.

Purpose of Compliance :

The audit was conducted not only to ensure adherence to compliance requirements but also to enhance the institution's overall IT security framework. By aligning IT policies with NIST SP 800-171, Illinois Institute of Technology ensures that it is on the forefront of protecting its digital assets against emerging threats and vulnerabilities, thus safeguarding its infrastructure and data across various departments and services.

Findings of Fact

Configuration and Baseline Standard

1. Policy Coverage
    - The policy covers multiple technology platforms and specifies the use of third-party benchmarks, which have been provided by CIS for initial configuration. It also covers the use of separate testing and production environments to test any new installations. The policy fails to explicitly document how the configurations are enforced.
2. Alignment with NIST SP 800-171
    - The policy properly documents Baseline Configurations in accordance with sections 3.4.1[a] through 3.4.1[c] of the NIST SP 800-171. It satisfies the basic requirements of the respective sections. While not required, it would be optimal to explicitly map controls to the specified controls in NIST SP 800-171 to further strengthen compliance.
3. Changelog
    - The policy fails to provide any procedures to properly record changes in Baseline Configurations
4. Responsibilities
    - The policy successfully assigns proper responsibility for the Configuration and Baseline standards to the Office of Technology Services (OTS). The policy, however, fails to document detailed accountability mechanisms and instead abstracts them to the Acceptable Use Policy (AUP).
5. Review and Update Measures
    - The policy dictates that the Configuration and Baseline standards are to be reviewed and updated annually. Which, while being in compliance with NIST SP 800-171, is suboptimal and should be changed to bi-annual reviews. It mentions that dynamic updates are to be done as required if any new threats arise, which need to be addressed immediately. The policy fails to document the procedures to integrate these dynamic updates into the configurations.
6. Training and Awareness
    - The policy fails to provide any details on training and awareness programs relating to maintenance and updates for Baseline Configurations.

Configuration Management Plan

1. Scope and Objectives:
    - The CMP is designed to maintain system integrity and availability through meticulous configuration management practices. Which aligns with the protection requirements specified by NIST SP 800 standards.
2. Policy Compliance:
    - CMP follows NIST SP 800 guidelines well, addressing policy creation, documentation, implementation, and enforcement mechanisms thoroughly.
3. Asset Identification and Inventory:
    - The CMP effectively identifies and catalogs all relevant hardware, software, and other critical assets by NIST SP 800 requirements.
4. Configuration Baselines:
    - Baseline configurations for various systems and components are established and regularly updated, ensuring alignment with NIST SP 800 criteria.
5. Change Management:
    - The processes for managing changes are robust, incorporating thorough control measures, approval processes, and detailed documentation as per NIST SP 800 recommendations.
6. Configuration Monitoring:
    - Configuration changes and deviations from established baselines are effectively monitored using a combination of automated tools and manual checks, aligning with NIST SP 800 recommendations.
7. Vulnerability Management:
    - The CMP's vulnerability management practices include comprehensive assessments, timely patching, and effective remediation, conforming to NIST SP 800 guidelines.
8. Incident Response:
    - The CMP is well-prepared to handle configuration-related issues during incident response activities, ensuring quick identification and resolution in line with NIST standards.
9. Documentation and Reporting:
    - Documentation within the CMP is thorough and accurately reflects all procedures, plans, and reports as required by NIST SP 800 standards.
10. Training and Awareness:
    - Provisions for ongoing training and awareness about configuration management practices are included in the CMP, aligning with NIST SP 800 recommendations.

System, Services and Asset Lifecycle Management Plan

1. Lifecycle Management
    - The plan meticulously outlines procedures for managing IT assets from the initial acquisition through to their final disposal. This includes the procurement processes, deployment strategies, operational handling, maintenance routines, and eventual decommissioning or renewal. By systematically documenting each phase, the plan ensures that all IT assets are managed consistently and securely, minimizing risks throughout their operational life.
2. Roles and Responsibilities
    - The policy defines roles and responsibilities for all stakeholders involved in the lifecycle management of IT assets. This clear delineation ensures that asset owners, IT management, and other stakeholders understand their specific duties and accountability. Such structuring not only facilitates efficient asset management but also reinforces adherence to security protocols, thereby enhancing organizational governance.
3. Security and Privacy Controls
    - Security controls are documented within the plan, covering the complete spectrum of asset management. These controls include physical security measures, access controls, cybersecurity policies, and privacy considerations. Enforcement mechanisms are clearly specified along with protocols for periodic security assessments to evaluate the efficacy of these controls and make necessary adjustments in response to evolving threats.
4. Monitoring and Auditing
    - To maintain high standards of compliance and operational integrity, the plan mandates annual reviews and detailed audits of the asset lifecycle processes. These reviews are designed to ensure continuous alignment with organizational goals and compliance frameworks, including NIST SP 800-171. Auditing procedures are comprehensive, focusing on both procedural adherence and the effectiveness of implemented controls.
5. Compliance with NIST Standards
    - The asset lifecycle management approach is tailored to align with the NIST SP 800-171 requirements, with a strong emphasis on configuration management. This alignment ensures that all IT assets are managed in a manner that adheres to federal standards for protecting Controlled Unclassified Information (CUI), thus reinforcing the institution's commitment to national security guidelines.
6. Data Protection Measures
    - Policies for data protection are integrated into the asset management framework, including rigorous data integrity checks and advanced encryption protocols for data at rest and in transit. These measures ensure the security and privacy of critical information throughout its lifecycle, protecting against unauthorized access and data breaches.
7. Systematic Security Review

  - Regular security reviews are institutionalized within the plan to ensure ongoing compliance with both internal standards and external regulations such as NIST SP 800-171. These reviews help identify and rectify security vulnerabilities, thereby enhancing the overall resilience of IT systems against cyber threats.

8. Documentation and Record Keeping
   - Extensive documentation and record-keeping practices are emphasized, covering all aspects of asset management from initial procurement to final disposal.This ensures an auditable trail that facilitates compliance checks and supports transparency in asset management operations .
9. Asset Inventory Management
   - A detailed asset inventory system is maintained, cataloging IT assets by type, sensitivity, and importance.This system is critical for effective risk management and security planning, allowing for targeted security measures based on the criticality and data sensitivity of assets .

Patch Management Policy

The Patch Management Policy outlines the responsibilities of application and system owners regarding patch management. As reviewed, the checklist audit document for the university's Patch Management Policy aligns with several requirements outlined in SP 800-171A and SP 800-171 Rev.2, which addresses the protection of Controlled Unclassified Information (CUI) in non-federal systems and organizations. The following is how it aligns with the SP 800-171A requirements:

- **Responsibilities:** Both documents highlight responsibilities that system owners and asset owners have regarding patch management so that there is reduction in security risks associated with having outdated software in operation.

- **Deployment Timeline:** Both documents have a time frame that they specify for deploying security patches. Illinois Institute of Tech requires that deployment be done within 30 days of release, a requirement satisfied for timely patching in SP 800-171 Rev.2.

- **Testing:** Both documents highlight how important it is for proper testing before deploying patches into production environments. This enables the patches to not introduce new vulnerabilities or disrupt system functionality.

- **Review:** Both documents allow for the periodic review and updates to patch management policy.

Encryption Standard Policy

1. **Encryption Standard Description**
    - The plan sufficiently covers the encryption standard required to maintain the protection of CUI, which includes the Encryption Requirements, Legal Recommendations, and Encryption Mechanisms. The policy meets the encryption requirements set forth by NIST for the protection of CUI.
2. **Roles and Responsibilities**
    - The policy properly divides tasks amongst its required roles, ensuring that no single role has access to the keys, data, and audit logs. The policy sufficiently describes the roles that individuals would be assigned and the responsibilities of those roles.
3. **PKI and KMS Description**
    - The policy properly describes how to manage both internal and external PKI/KMS solutions. This includes describing the requirements and risk management methods for both solutions. It comprehensively describes the necessary information to manage both solutions effectively.
4. **Pre-Share Keys and Certificate Validation**
    - The policy describes the necessary compliance requirements when using pre-shared keys and the minimum requirements that applications using certificates must meet. These are in line with the standards set forth by NIST to ensure that keys and certificates are used appropriately for authentication.

Conclusions and Recommendations

Configuration and Baseline Standard

1. **Baseline Configuration Enforcement**
    - Recommendation: While the current policy only has the bare minimum Baseline Configurations that are provided by the vendors, it needs to strengthen these configurations. It also needs to properly document how enforcement is done and what methods are used to enforce these configurations.
    - Action Steps:
        - Document any existing enforcement protocols in use or develop enforcement protocols that automatically verify compliance.
2. **Accountability**
    - Recommendation: While the policy abstracts the accountability procedures to the Acceptable Use Policy (AUP) it is advisable to draft specific accountability procedures for Configuration and Baseline Standards enforcement.
    - Action Steps:
        - Define accountability procedures in the existing Configuration and Baseline Standard policy.
3. **Change Logging**
    - Recommendation: Any changes that have been made to the Baseline Configuration should be properly recorded and a trail should be maintained.
    - Action Steps:
        - Define procedures to log any changes that have been made to the Baseline Configuration.

4. **Dynamic Update Procedures**
    - Recommendation: Properly document the procedures in place to integrate emergency updates into the Baseline Standards.
    - Action Steps:
        - Create and document procedures to integrate emergency updates to new cyber threats to the systems in use.
5. **Training and Awareness Programs**
    - Recommendation: Illinois Tech should create proper training and awareness programs for Configuration and Baseline Standards Management.
    - Action Steps:
        - Design training modules that contain information regarding Baseline Configurations and their importance to security, and the role of every stakeholder involved.
        - Schedule bi-annual training sessions to ensure employees are consistently aware of their responsibilities.
6. **Review and Updates**
    - Recommendations: The review frequency of the Configuration and Baseline Standard policy should be increased to bi-annual reviews.
    - Action Steps:

  - Amend the policy to enforce bi-annual reviews of the baseline configuration standards.

Configuration Management Plan

1. Improving Document Structure and Accessibility

- Recommendation: Facilitating the model for easy comprehension is crucial to ensure access and comprehend the policies of all stakeholders within them.
- Action Steps:
    - Simplify Language: Rewrite the configuration management documents using simple, clear language to make them accessible to all stakeholders, not just technical experts.
    - Use Visual Aids: Introduce diagrams, flowcharts, and other visual aids to illustrate complex concepts and processes, making them easier to understand.
    - Decentralize Access: Ensure that the documents are easily accessible to all stakeholders by hosting them on a central, easily navigable platform.

2. Enhance Policy Detailing and Compliance

- Recommendation: Although the document covers all required areas, adding more specifics about enforcement mechanisms for compliance with these policies would strengthen its utility and effectiveness.
- Action Steps:
    - Specify Enforcement Protocols: Clearly define and document specific enforcement protocols for each policy, outlining the steps to be taken when policies are not followed.
    - Define Roles and Responsibilities: Clarify which roles are responsible for monitoring compliance and enforcing policies, ensuring there is no ambiguity.
    - Implement Monitoring Tools: Utilize technology to monitor compliance automatically, providing real-time alerts when deviations occur.

3. Asset Identification and Inventory Management

- Recommendation: The plan's thorough approach to asset management meets NIST standards but could benefit from continuous advancement in inventory accuracy to keep pace with changing technology and security needs
- Action Steps:
    - Update Inventory Processes: Regularly update and refine inventory processes to incorporate advances in technology and shifts in security demands.
    - Automate Inventory Management: Implement automated systems to enhance the accuracy and efficiency of tracking assets, reducing the risk of human error.
    - Frequent Asset Audits: Schedule more frequent audits of the asset inventory to ensure all items are accurately accounted for and properly classified.

4. Configuration Baselines and Change Management

- Recommendation
  The current practices are strong and meet NIST standards, but improving real-time tracking and analysis of changes would offer deeper insights and better control over system configurations.
- Action Steps:
  - Implement Real-Time Tracking Systems: Deploy advanced real-time tracking systems that can immediately detect and log changes in system configurations. This will provide instant visibility into any modifications made.
  - Enhance Data Analysis Tools: Invest in sophisticated data analysis tools that can interpret change logs and track trends over time. These tools will offer deeper insights into the impacts of changes and help predict potential issues before they occur.
  - Integrate with Incident Management: Connect the real-time tracking system with the institution’s incident management platform. This integration will allow for swift response to unauthorized changes, enhancing security and control.

5. Monitoring and Reporting

- Recommendation: Although the current monitoring methods work well, using more automated, real-time tools would enhance our ability to respond quickly and detect threats more effectively.
- Action Steps:
  - Upgrade to Real-Time Monitoring Tools: Invest in and deploy real-time monitoring software that can detect and alert staff to system changes and potential threats as they happen.
  - Automate Reporting Processes: Implement automated systems to generate reports based on monitoring data, ensuring that information is consistently recorded and easily accessible for analysis.
  - Enhance Threat Detection Capabilities: Incorporate advanced threat detection technologies into the monitoring tools to identify and respond to security risks more effectively.

6. Vulnerability Management and Incident Response

- Recommendation: The methods for managing vulnerabilities and incidents are proactive and detailed, but using ongoing assessment tools more extensively and conducting more regular response drills could improve these processes.
- Action Steps:
  - Expand Use of Continuous Assessment Tools: Implement advanced continuous vulnerability assessment tools that can constantly scan and analyze the IT environment to identify and address vulnerabilities as they emerge.
  - Increase Frequency of Response Drills: Schedule more frequent incident response drills to ensure that response protocols are well-practiced and team readiness is optimal.

    - Integrate Assessment Tools with Response Protocols: Ensure that the continuous assessment tools are fully integrated with incident response systems, allowing for a seamless transition from detection to action.

7. Training and Awareness

- Recommendation: Including more hands-on scenarios and interactive content in these training programs could make them more effective.
- Action Steps:
    - Automate Document Updates and Notifications: Utilize automation within the document management system to update documents and notify relevant stakeholders of changes or necessary reviews, enhancing real-time information sharing.
    - Train Staff on System Use: Conduct training sessions for all relevant personnel on how to use the new document management system effectively, focusing on how to upload, retrieve, and manage documents.
    - Regular Audits of Document Practices: Schedule regular audits to ensure that the documentation practices meet compliance standards and that the document management system is being used effectively.

System, Services and Asset Lifecycle Management Plan

1. **Enhance Security Control Enforcement**
    - Recommendation: While security controls are well-documented, there is a need for clearer enforcement details and specific methods, especially concerning asset disposal and data sanitization.
    - Action Steps:
        - Define clear enforcement protocols for each security measure.
        - Document specific sanitization methods for different types of assets to ensure data security even after asset disposal.
2. **Improve Compliance Adaptability**
    - Recommendation: Although the plan includes mechanisms that imply adaptability to new security threats and technological changes, these mechanisms should be explicitly detailed and formalized.
    - Action Steps:
        - Develop a formal change management process within the lifecycle management plan that includes periodic security assessments.
        - Set clear triggers for reviews and updates, such as new security threats or technological innovations.
3. **Establish Compliance Monitoring Mechanisms**
    - Recommendation: The plan currently lacks specific mechanisms for monitoring compliance with the lifecycle management policy. Establishing these will ensure continuous adherence and quick identification of deviations.
    - Action Steps:
        - Implement real-time monitoring tools to track compliance.
        - Develop a dashboard for ongoing oversight of lifecycle management activities and their compliance status.
4. **Develop Effectiveness Metrics and Reporting**
    - Recommendation: The absence of specific metrics to measure the effectiveness of asset lifecycle management is a notable gap. Developing and implementing these metrics would allow for better tracking and management.
    - Action Steps:
        - Identify key performance indicators (KPIs) for asset lifecycle management.
        - Regularly review these metrics and report the findings to senior management to inform decision-making and policy adjustments.
5. **Formalize Documentation and Record Keeping**
    - Recommendation: Enhance the current documentation and record-keeping practices to ensure they not only remain systematic but also incorporate advanced digital solutions for better management and retrieval.
    - Action Steps:
        - Implement a centralized document management system that aligns with Illinois Tech policies and ensures compliance with regulatory requirements.

- Train staff on the importance of meticulous documentation and the use of the new system.

Patch Management Policy

1. **Policy Coverage**
   - Recommendation: Review whether the University's Patch management Policy adequately covers all aspects of patch management which might aspects like timelines, responsibilities, review processes.
2. **Alignment with NIST SP 800-171**
   - Recommendation: Check whether the University's Patch Management Policy goes hand in hand with requirements specified by NIST SP 800-171 as well as NIST SP 800-171 Rev. 2 for protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations.

3. Responsibilities and Accountability

- Recommendation: Review the policy to ensure responsibilities are clearly distinguished as well as accountability measures.

4. Timelines

- Recommendation: Verify that the policy has timelines addressed for deploying security patches.

5. Security Patch Monitoring and Notification

- Recommendation: Review ways of monitoring patch releases, security vulnerabilities.

6. Documentation and Record-keeping

- Recommendation: Review requirements that can be used for documenting patch management activities such as the records for patch releases, compliance with NIST SP 800-171, vulnerability checks, recommendations done, test results and auditing trail.

7. Training and Awareness procedures

- Recommendation: Assess procedures in place for educating personnel on patch management, personnel roles as well as their responsibilities, mechanisms for organizational systems and data protection.

Encryption Standard Policy

1. **Improve Accountability Procedures**
    - Recommendation: The policy defers the accountability process to the Acceptable Use Policy (AUP), but role-specific accountability procedures would be preferred
    - Action Steps: Set well-defined role-based accountability procedures within the Encryption Standard Policy.
2. **Improve Policy Review Description**
    - Recommendation: The policy simply states that the review needs to be done annually, but it would benefit from well-defined steps that describe what is required in the annual review.
    - Action Steps: Create a proper review process guideline to ensure that the document review is done in a systematic manner.
3. **Define Exception Handling Procedures**
    - Recommendation: The policy delegates the handling of any standard practice exceptions to CTS but should have proper guidelines for what actions are to be taken in case of these exceptions.
    - Action Steps: Create suitable guidelines that define what steps are to be taken in case of any exceptions to the defined standards.

Appendix

Scope Document

Objectives

- **Verify Compliance** : Ensure all specified IT policies comply with the NIST SP 800-171 standards, particularly regarding the protection of Controlled Unclassified Information (CUI).
- **Identify Gaps** : Find any policy compliance gaps that might compromise the security of CUI and other sensitive data the organization manages.
- **Documentation and Procedures** : Evaluate the appropriateness of current documentation and procedural directives as outlined in the policies.

Key Areas of Focus

1. **Patch Management Policy**
   - Examine the patch management procedures to ensure that they meet the time and thoroughness requirements for security patch application and testing as outlined in NIST guidelines.
   - Ensure that roles and responsibilities related to patch management are clearly articulated and align with best security practices.
2. **Encryption Standard**
   - Examine encryption technologies and their implementation in various IT settings to ensure they meet NIST specifications for data at rest and in transit.
   - Confirm that key management practices are robust and comply with NIST's guidelines for key generation, usage, storage, and destruction.
3. **Configuration and Baseline Standard**
   - Examine the Configuration and Baseline Standards to ensure that they align with NIST specifications.
   - Examine the processes for updating and monitoring these baseline standards, making sure they include mechanisms for tracking, reviewing, and auditing these modifications.
4. **Configuration Management Plan**
   - Examine the configuration management processes to verify they adequately protect system configurations from unauthorized changes, in line with NIST standards.
   - Evaluate the methods used for establishing the initial configuration, making modifications to the established configuration, and conducting audits of the configuration.
5. **System Services and Asset Lifecycle Management Plan**
   - Investigate how the lifecycle of system services and assets is managed from acquisition to disposal, ensuring compliance with NIST's security and privacy controls.
   - Review the integration of security considerations throughout the system development lifecycle (SDLC) and asset management procedures.

Methods of Examination

- Perform a document review with thorough analysis of all policy documents and their compliance with **NIST SP 800-171**.
- Utilize checklists and other audit tools to verify adherence to NIST guidelines across all policy domains.

Checklists

Configuration and Baseline Standard Audit Checklist

Area of Evaluation	Checklist Item	Compliant (Yes/No)	Comments/Recommendations
Documentation of Baseline Configuration	Are the Baseline Configurations properly documented?	Yes	Only the vendor suggested configurations are documented and currently enforced.
Roles and Responsibilities	Are responsibilities and roles clearly defined within the policy?	Yes	Responsibilities have been defined briefly. They need to be defined explicitly and accountability measures are referenced to another policy.
Compliance with External Regulations	Are the Baseline Configurations in compliance with NIST SP 800-171?	Yes	Compliant with NIST SP 800-171. Some areas need improvement.

Review and Update Procedures	Are there established procedures for regular reviews and updates of the Baseline Configurations?	Yes	Annual reviews are mandated. However, reviews should be done on a bi-annual basis.
	Is there a mechanism in place to adapt the Baseline Configuration to new threats?	Yes	The mechanisms are mentioned but are not explicitly defined.
	Are the methods to integrate dynamic changes to the configurations defined?	No	The methods to integrate dynamic changes into existing Baseline Configurations are not defined

Configuration Management Plan

Area of Evaluation	Checklist Item	Complaint (YES/NO)	Comments/Recommendations

Configuration Management Policy	Does the policy comprehensively outline roles, responsibilities, and the scope of configuration management?	Yes	IIT’s Configuration Management policy is detailed in specifying the roles and responsibilities duties of system administrators, IT security staff, and end-users in managing configurations across different departments and levels.
	Does the policy include enforcement mechanisms clearly defined and adequate?	Yes	Regular compliance checks and audits, along with penalties for not following them, help make sure everyone sticks to the set configuration management practices.
Baseline Configuration Procedures	Are baseline configurations defined for all critical system components?	Yes	Critical components like network devices, servers, and software are set up following industry best practices and vendor advice.
	Is there a process for updating baseline configurations when system changes occur?		IIT's method includes having a CCB to review changes, testing them in a safe setting, and documenting everything before implementation.

System Inventory Procedures	Are there any established procedures for maintaining an accurate system inventory?	Yes	IIT uses automated tools to keep a detailed inventory of all its IT assets, tracking hardware and software across the campus network.
System Security and Configuration Management Plans	Is the system inventory regularly updated, and are these updates documented?	Yes	IIT's inventory is updated instantly using automated systems, with all changes recorded centrally and checked every three months by the IT department. Top of Form
	Does the System Security Plan specifically mention practices for managing system settings?	Yes	The System Security Plan incorporates practices for managing system settings to align with the overall security strategy and meet the requirements for protecting the sensitive information of CUI.
Inventory and Change Control Records	Are the security controls defined in the plan aligned with baseline configuration requirements?	Yes	All security measures are set up to uphold basic system settings, including access rules, malware defense, and data encryption.

	Are system inventory records complete and reflective of the current state of system assets?	Yes	Inventory records are thorough, showing the latest details and conditions of all system assets as confirmed by the most recent quarterly audit.
	Do change control records thoroughly track each modification, including the reasons for changes, approvals, and reviews after changes are made?	Yes	Every system change is recorded in CB with details about what was changed, why, who approved it, and a review of the outcomes after the change

System, Services and Asset Lifecycle Management Plan

Area of Evaluation	Checklist Item	Compliant (Yes/No)	Comments/Recommendations
Documentation of Lifecycle Management	Is there a comprehensive lifecycle management plan documented?	Yes	Plan is well-documented.

	Does the documentation include all phases of the lifecycle (acquisition, use, maintenance, and disposal)?	Yes	Covers all lifecycle phases comprehensively.
Roles and Responsibilities	Are responsibilities and roles clearly defined within the policy?	Yes	Roles are well-defined across different stakeholders.
	Are these roles distributed adequately among asset owners, IT management, and other stakeholders?	Yes	Adequate distribution and definition of roles.
Security Measures	Are security controls for protecting assets throughout their lifecycle documented and enforced?	Yes	Security controls are documented, though specific enforcement details could be expanded.

	Does the plan include specific security measures for asset disposal and data sanitization?	Yes	Includes disposal and sanitation but could detail specific methods more clearly.
Compliance with External Regulations	Does the lifecycle management comply with relevant industry regulations and standards (e.g., NIST SP 800-171)?	Yes	Complies with NIST SP 800-171, some areas might require updates to stay current with latest standards.
Review and Update Procedures	Are there established procedures for regular reviews and updates of the lifecycle management plan?	Yes	Annual reviews are mandated.
	Is there a mechanism in place to adapt the lifecycle plan based on new security threats or technological changes?	Yes	Adaptive mechanisms are implied, though not explicitly detailed.

Asset Inventory Management	Is there a complete and up-to-date inventory of all assets?	Yes	Document specifies inventory management systems.
	Are the assets classified according to their sensitivity and importance?	Yes	Asset sensitivity classification is implied in management protocols.
Security Patch Management	Are procedures in place for timely application of security patches?	Yes	Referenced to a separate Patch Management document.
	Are patch management responsibilities clearly assigned?	Yes	Clearly assigned within the referenced document.
Monitoring and Auditing	Are mechanisms established for monitoring compliance with the lifecycle management policy?	No	Specific compliance monitoring mechanisms are not detailed.

	Are regular audits conducted to assess the effectiveness of asset management practices?	Yes	Annual audits are part of the inventory management process.
Metrics and Reporting	Are metrics used to measure the effectiveness of asset lifecycle management?	No	No specific metrics for effectiveness measurement are mentioned.
	Are these metrics regularly reviewed and reported to senior management?	No	Lack of metrics means no reporting is detailed.
Documentation and Record Keeping	Are records of asset management activities (acquisition, maintenance, disposals) maintained systematically?	Yes	Detailed record-keeping practices are outlined.

	Do documentation and records comply with Illinois Tech policies and regulatory requirements?	Yes	Complies with institutional policies and regulations.

Patch Management policy checklist

Area of Evaluation	Checklist Item	Compliant (Yes/No)	Comments/Recommendations
Patch Management	Patch Management Policy covers all necessary aspects of patch management?	Yes	complies
Roles	Responsibilities, roles, security deployment timelines, tests, and review processes clearly defined within policy?	Yes	complies
Responsibilities	Responsibilities for patch management clearly distinguish among asset owners, management, and other relevant stakeholders?	Yes	complies

Timelines	Policy produces appropriate timelines for deploying security patches?	Yes	complies
Procedures	Procedures well documented for testing patches prior to deployment into production environments?	No	Document does not show procedures for tests
Mechanisms	Mechanisms in place for monitoring patch release notifications as well as staying informed about security vulnerabilities?	No	No formal method to stay informed of vulnerabilities
	Mechanisms established for monitoring compliance with the Patch Management Policy?	No	No formal method to monitor compliance with NIST SP 800-171
Metrics	Metrics used for regular audits, assessments, or patch deployment for compliance monitoring?	No	Use metrics for quantitative analysis
Records	Records of patch deployment, testing results, and audit trails maintained according to Illinois Tech policies and regulatory requirements.	Yes	Policy document complies

Encryption Standard Policy Checklist

Area of Evaluation	**Checklist Item**	**Compliant (Yes/No)**	**Comments/Recommendations**
Encryption Standard Policy	Encryption Standard Policy cover all requirements, mechanisms, and legal recommendations?	Yes	In compliance
Roles and Responsibilities	Roles And Responsibilities well-defined and documented?	Yes	In compliance
	Responsibilities for each role are well segregated to ensure one person doesn't have access to keys, data, and audit logs?	Yes	In compliance
	Role-specific accountability procedures in place in case of any violations?	No	Set well-defined role-based accountability procedures within the Encryption Standard Policy.
Procedures	PKI/KMS solutions well defined for both	Yes	In compliance

	internal and external suppliers?		
	Minimum requirements defined for using pre-shared keys and for using certificates for validation?	Yes	In compliance
	Procedure for handling of exceptions to the listed standard well described?	No	Create suitable guidelines that define what steps are to be taken in case of any exceptions to the defined standards.
Review	Timeline for review of the document set clearly?	Yes	In compliance
	Guideline for the review process described to ensure systematic reviews?	No	Create a proper review process guideline to ensure that the document review is done in a systematic manner.