Integrated Information Technology Services

POLICIES AND PROCEDURES

Change and Patch Management Policy

POLICY:

Utica University is dedicated to maintaining the stability, security, and integrity of its information systems and operational processes. This Change and Patch Management Policy establishes a structured framework for the planning, review, approval, implementation, and documentation of changes to the university's IT infrastructure and systems. All changes must be reviewed and approved by the IITS (Integrated Information Technology Services) directors before implementation.

SCOPE:

This policy applies to all changes to Utica University's IT systems, applications, networks, and infrastructure. It covers modifications that may impact security, operations, performance, compliance, or availability, including hardware upgrades, software updates, configuration changes, and new system deployments.

REASON FOR POLICY:

To ensure that changes to IT systems are:

- Consistent with Utica University's operational goals and security standards.
- Effectively planned and tested to minimize potential disruptions and risks.
- Documented to support accountability, compliance, and future reference.
- Reviewed and approved by the appropriate authority to maintain system integrity and security.

DEFINITIONS:

- **Change:** Any modification to the IT infrastructure, systems, applications, or processes, including updates, patches, upgrades, or deployments.
- **Change Management Process:** A formal procedure for evaluating, approving, and documenting changes to IT systems.
- **Change Request (CR):** A IITS Ticket proposal for a change, detailing its purpose, scope, potential impact, and implementation plan.

PROCEDURE:

1. **Change Request Submission:**
    - Individuals or teams proposing a change must complete a Change Request (CR) form, detailing the purpose, scope, potential risks, impact, and rollback plan.
2. **Review and Risk Assessment:**
    - The CR is reviewed by the relevant stakeholders, including IT staff, data owners, and business units, to assess risks, benefits, and potential impact on university operations.
3. **Approval:**
    - All proposed changes must be reviewed and approved by the IITS directors before implementation.
    - High-impact changes may require additional approval from senior leadership.
4. **Testing:**
    - Proposed changes must be tested in a controlled environment to ensure functionality and compatibility with existing systems.
5. **Implementation:**
    - Approved changes are implemented following a predefined plan, including schedules to minimize disruption.
    - A rollback plan must be in place in case the change causes unforeseen issues.
6. **Documentation:**
    - Details of the change, including approvals, testing results, and implementation outcomes, must be documented and stored for future reference.
7. **Post-Implementation Review:**
    - After the change is implemented, a review is conducted to ensure its success and address any issues.
8. **Automatic Approval:**
    - Critical and Monthly updates should be reviewed and tested before implementation in production. So long as no issues are presented, they are exempt from this review and shall automatically be approved to be installed.

RESPONSIBILITY:

- **IITS Directors:** Responsible for reviewing and approving all proposed changes to IT systems and ensuring adherence to this policy.

- **Information Security Officer (ISO):** Evaluates the security implications of proposed changes and ensures compliance with security standards.
- **Change Proposers:** Responsible for submitting comprehensive CRs, conducting testing, and executing changes in accordance with this policy.
- **IT Staff:** Ensures changes are implemented following approved plans and with minimal disruption.

ENFORCEMENT:

Non-compliance with this policy may result in disciplinary action, including revocation of system access, termination of employment, or termination of vendor contracts. Unauthorized changes will be reported to the IITS directors and senior leadership for further action.

RESOURCES/QUESTIONS:

For more information, contact the Utica University IITS Help Desk, which can be reached via telephone at (315) 792-3115. See also the Responsible Use of University Computing Resources policy.

Please note that other Utica University policies may apply or be related to this policy. To search for related policies, use the Keyword Search function of the online policy manual.

_____

Todd Pfannestiel, President Date

Effective Date:
Promulgated:

Last Revised:
Promulgated: