29.01.99.K1.410 SIS Change Management Standard Administrative Procedure

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: March 28th, 2019
Next Scheduled Review: March 2024

Purpose

The purpose of this procedure is to establish the procedures for initiating and recording changes to the Banner Student Information System.

Audience

This procedure applies to employees requiring modifications or updates to TAMUK's student information system.

Applicability

This procedure applies to the Student Information System and associated information resources. Any request for modification to compiled code including, but not limited to application upgrades, patches, and user requested modifications, modification to data outside of Banner Admin Pages or Self Service, or other changes that affect the application must be submitted and approved prior to the change being implemented.

Definitions

1. **Banner**: TAMUK's Student Information System, Ellucian Banner.
2. **Banner Admin Pages**: This is the administrative interface into Banner.
3. **Change**:
    - Any implementation of new functionality;
    - Any modification to data outside of the prescribed user interface;
    - Any modification of existing functionality;
    - Any removal of existing functionality.

4. iTech support site: The iTech help desk ticketing system site accessible at http://support.tamuk.edu.

Student Information System Change Management Procedure

All requests for changes described above must be submitted to iTech in the form of a change request through the iTech support site. Approval of all changes to Banner must be approved through the Banner Users Group (See Appendix A for details). To ensure a successful implementation of the change, preparation will be required.

1. Preparation may include:
    a. Review of results of previously implemented changes to prevent repetitive mistakes or negative impacts.
    b. Determination of the length of time to implement the change to assure it can be accomplished within the weekly maintenance window.
    c. Assessment of the impact to other systems.
    d. Assessment of the risk associated with the change implementation to minimize the risk of service disruption.
    e. Development of a back-out/rollback plan in the event that the change needs to be reversed.
        i. The plan must include the identification of a back-out/rollback window which is the time period in which the decision to reverse the change can safely be made.
    f. Confirmation that the changes will not negatively impact the overall system security.
    g. Approval from the module owner affected by the implementation of the change
2. Review/approval may include:
    a. Determination of the level of control necessary based on inherent risk. Typically, the higher the risk the greater the level of control required. Controls include, but are not limited to, levels of approval, types of testing performed, length of review time, and consultation with subject matter experts.
    b. Review of change-related details, including functional review where appropriate by the individual(s) responsible for approving the change.
    c. Review of logs for previous change implementations.
    d. Formal, documented approval or rejection of the change.
    e. For changes involving code revision, review and approval shall be performed by someone other than the developer.
        i. For emergencies, management may make an exception to the review process.

3. Notification must be given to users in a timely manner, including relevant details that would not negatively impact the security of the information resource, such as time and date, nature of the change, and time needed for implementation. The method of notification should be appropriate to the environment and the user base, and may include email or an announcement posted in the portal.
4. Post-implementation review may include:
    a. Verification that the change occurred.
    b. Testing of the system post-change.
    c. Resolution of any problems, if possible.
    d. Decision on whether to initiate back-out plan.
    e. Analysis of any issues or complications.

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

Appendix A: Procedures for Change Request

1. User initiates a change request via the iTech support site, or one is initiated on their behalf.
2. Change is reviewed by iTech personnel and an item placed on the Banner Users Group agenda for the next available meeting.
3. After discussion by the Banner Users Group, change tasks are created, if needed, under the change request on the support site and approvers assigned to each task and the change request.
4. Once all tasks have been implemented into the Banner TEST environment by iTech and approved by the appropriate approvers a scheduled date will be set for implementation of the change in the Banner PROD environment.
5. If calculated downtime exceeds the length of the weekly maintenance window, the scheduled outage needs to be communicated to the campus community by the chair of the Banner Users Group, taking into account important academic and administrative dates and the effects the downtime may have.
6. Once changes are implemented in the Banner PROD environment, user acceptance testing is performed by functional staff and communicated to iTech Banner staff.
7. The change request is updated to reflect the success or failure of the applied change. Lessons learned from the change may be included in change notes by iTech staff, if necessary.

References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
3. Computer Security Act of 1987
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
6. Foreign Corrupt Practices Act of 1977
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
14. Texas Government Code, Section 441

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404