Status Active PolicyStat ID 19185659

Origination	10/2025	Chapter Lead	Brooke Quinones: HR Admin
Last Approved	10/2025	Policy Area	Chapter 3 General Institution
Effective	10/2025		
Last Revised	10/2025		
Next Review	10/2031		

AP 3731Information Security Internally Developed Systems Change Control

1. PURPOSE AND SCOPE

The objective of this Administrative Procedure is to ensure a standardized method for handling changes to District internally developed systems. Change control promotes the stability of the environment, which is essential to its security and integrity.

This is one of a series of information security Administrative Procedures designed to protect District information systems. The District Information Technology (IT) department has a district-wide fiduciary responsibility to set, maintain, and ensure the provisions of this regulation. District IT accomplishes this through collaborative engagement with the campus Technology Services departments.

A. **Applicability**
This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, such as short-term (temporary) staff, substitutes, professional experts, Federal Work Study students, and student help who are employed by and volunteers who assist the District for the purpose of meeting the needs of students.

B. **Applicability to External Parties**
This Administrative Procedure applies to all external parties, including but not limited to District business partners, vendors, suppliers, service providers, and other third-party entities with access to District networks and system resources.

C. **References and Related Procedures**
Please refer to the Information Security Administrative Procedures for additional information, references, and definitions:

2. CHANGE CONTROL

A change is any modification or enhancement to an existing production system. Modifications can be

updates to existing data, functionality, or system processes. The District IT department shall adhere to industry best practices in the development and maintenance of all internally developed systems.

A. **Change Roles**
The following roles have been established to guide the Change Management process for internally developed applications:

- Release Manager: Oversees the change being released into production.

- User: the individual or entity initiating a change, which may be either an internal District employee or contractor or an external organization.

- Product Owner: the role that qualifies and prioritizes customer Change Requests. The Product Owner may represent interests within a specific organizational entity.

- Prioritization Committee: one or more organizational bodies that review and prioritize Change Requests submitted by Product Owners or the user community.

- Quality Assurance Team: the internal department to test developed changes prior to introducing them into production. This group must be independent of the development group.

- Release Team: Internal team designed to schedule and implement changes into production.

- Development Team: the internal District group responsible for implementing and/or delivering the Change Requests.

B. **Process Tools**
The primary tools used to manage Change Requests are the District-wide Service Desk system for project management and an Application Lifecycle Management tool for logging, backup, and integrity monitoring.

C. **Change Requirements**
The basic requirements for Change Management are:

Changes that are part of the production environment must follow defined procedures by submitting a Change Request through the service desk system.

1) The User submits the Request.

2) The Request is reviewed by District IT, the relevant Product Owner, and further reviewed and prioritized by the Prioritization Committee.

3) Once approved by the Prioritization Committee, the development team schedules and implements the change.

4) All changes must be authorized by the appropriate management.

5) All changes to production software must be completely and comprehensively tested.

6) All required documentation associated with the changes must be included with the software delivery.

7) Program source code must be protected by restricting access to those within the Development team who have a need-to-know. Segregation of duties must be maintained.

8) Version controls for source code must be in place to maintain application integrity.

9) All change requests must be accompanied by back-out procedures to be used in the event of unexpected error conditions.

10) Roll-back execution conditions will be defined during the Project Release plan creation.

11) Production data should not be used for testing data unless it has been scrubbed. Where sensitive data must be used, the
development and test environments will remain isolated from external communication.

D. **Application Security Knowledge Transfer**
Changes related to new or significant implementation efforts should include a knowledge transfer of relevant security information from the Development team to the Network and Security staff and other interested parties.

E. **Payment Card Industry Considerations**
Refer to AP 3737 Information Security - Payment Card Industry Requirements (PCI).

Approval Signatures

Step Description	Approver	Date
Approved per Level 3 process in AP 2410	Brooke Quinones: HR Admin	10/2025