LOS ANGELES UNIFIED SCHOOL DISTRICT
POLICY BULLETIN

TITLE: Change Management for Critical Information Systems

NUMBER: BUL-106900

ISSUER: Soheil Katal, Chief Information Officer
Information Technology Division

James Thurmond, Director of IT Security
Information Technology Division

DATE: April 30, 2021

ROUTING
Central Offices

PURPOSE: The purpose of this Bulletin is to establish minimum requirements for planning, documenting, testing, and approving changes made to critical information systems to ensure the confidentiality, integrity, and availability of protected District information. This policy applies to all internal and external production information systems critical to District operations.

MAJOR CHANGES: This is a new Policy Bulletin.

BACKGROUND: The District is constantly focused on meeting the changing digital needs of students, parents, and employees, which means that the information systems they use must change at the same pace. Frequent and rapid changes to information systems, such as upgrades, bug fixes, and enhancements, can cause costly disruptions and prolonged downtime. To ensure the continuity of District operations that rely on critical applications, a District-wide standard for properly controlling and introducing changes to information systems is required.

DEFINITIONS:

Protected Information - Information protected by certain laws, classified under the "Information Protection Policy," BUL-1077.2, that includes personally identifiable information (PII), protected health information (PHI), and sensitive security information (SSI).

Sensitive Security Information - Information related to internal information security operations whose disclosure would harm the confidentiality, integrity, and availability of District assets.

Change – The addition, modification or removal of any information technology component that could affect the delivery of stable, reliable, and secure IT services. Some examples are:

- Hardware changes (e.g. installing a server)
- Software changes (e.g. patching an operating system)
- Application changes (e.g. adding additional features)
- Process changes (e.g. removing a step in an approval workflow)

Critical Information System - All Tier 1 systems listed in the District's Business Continuity Plan that must be restored within 24 hours or less after an interruption of service. These systems may support administrative or instructional operations, protect human life or property, or manage enterprise IT infrastructure that, if failed, can suspend core financial transactions, interrupt school instruction District-wide, cause significant injury or death, or compromise confidentiality, integrity, and availability of information assets. Examples include financial systems, learning management systems, fire safety systems, and security systems.

GUIDELINES: Each system owner is accountable for ensuring that a documented change management process is in place. This process should manage changes to information processing facilities (e.g. data centers, telecommunication rooms, etc.) and critical information systems. A documented change management procedure must be made available upon request to ITD Information Security to monitor compliance.

The change control process must be minimally defined and managed according to the following guidelines:

I. Initiation

A. Documentation

Proposed changes must be documented so that it is clear what changes are being made, what systems are being affected, the risk of implementation, when they are implemented, and who approved the change.

B. Risk Assessment

A risk assessment must be performed to evaluate the relative impact of proposed changes and calculate the probability of adverse outcomes. The system owner must establish a methodology for assessing the risk of proposed changes. A commonly used methodology is combining a few important operational factors into a single aggregate measure such as high, medium, or low. Some example risk factors may include:

- Impact (e.g. number of users or integrated systems)

- Urgency (e.g. how quickly the change needs to be addressed)
- Priority (e.g. how the change ranks against other requirements)

C. Communication
Changes must be properly communicated to all relevant stakeholders of the system(s), including business owners, system custodians, and when necessary, end users.

II. Review and Authorization

A. Approval Process
Changes must be reviewed and approved by the business owner. Additional approvals may be required depending on risk, complexity of the change, and stakeholders of the affected systems. The approval process should ensure that:

- roles and responsibilities are established
- changes are submitted by authorized users
- formal approval by the business owner is obtained before work to implement the change commences
- system owners accept changes prior to implementation

B. Security Review
Changes must be evaluated to ensure the availability of information and the critical systems that provide it can appropriately resist attacks and unauthorized access.

III. Planning and Scheduling

Prior to implementation, proposed changes must be planned, prioritized, tested, scheduled, and include roll-back procedures in case problems arise during implementation.

A. Planning
Implementation plans should detail the various tasks and the order in which they must be carried out to result in a successful deployment.

B. Scheduling
Proposed changes must be scheduled to occur at an appropriate time that minimizes interruption to school operations.

C. Testing
Testing must be conducted in a test environment that replicates the critical production system being changed. If a test environment is

not available, testing must be performed using methods that must be approved by IT Security that closely resemble the production environment to the greatest extent possible.

D. Roll-Back Procedure
Implementation plans must include procedures and responsibilities for aborting and recovering from unsuccessful changes or unforeseen events.

E. Exceptions/Emergencies
Provisions must be made to accommodate necessary changes in the event of emergencies that require an accelerated response, or exceptions to the normal change management process.

IV. Implementation and Closing

A. Documentation
Documentation of changes must be updated upon the completion of each change and retained for a period of at least five (5) years, in order to create an auditable trail of change requests.

Operating documentation, such as user guides or manuals must also be updated, when appropriate.

V. Validity & Document Management

The owner of this document is the Director of IT Security, who must check and, if necessary, update the document at least once a year. When evaluating the effectiveness of the document, the number of critical information systems without a documented change management process must be considered.

RELATED RESOURCES: BUL-1077.2 "*Information Protection Policy*" dated July 18, 2017

ISO/IEC 27001 standard, clauses A.12.1.2, A.14.2.4

ASSISTANCE: For assistance or further information please contact the Office of Information Security at information.security@lausd.net