ILLINOIS STATE POLICE DIRECTIVE
SRV-227, CHANGE MANAGEMENT OF COMPUTER SYSTEMS/APPLICATIONS

RESCINDS: New Directive	**REVISED:** 04-15-2024 **2024-021**
RELATED DOCUMENTS: SRV-201	**RELATED CALEA STANDARDS (6th Edition):** 11.4.4, 11.4.5, 12.1.4

I. POLICY

I.A. The Illinois State Police (ISP):

I.A.1. Will establish processes for the handling of changes to information technology (IT) resources ensuring an acceptable balance of risk and resource effectiveness and reduce the potential risk of disruption in services.

I.A.2. Is a client agency of the Department of Innovation and Technology (DoIT), and as such, while maintaining appropriate oversight, defers to DoIT to establish processes for the handling of changes to DoIT controlled/administered IT resources that ensure an acceptable balance of risk and resource effectiveness, and reduce the risk of potential disruption in services, where appropriate.

I.A.3. Will review and approve changes to all ISP controlled IT resources as set forth below.

I.B. The Change Request Form, weekly Change Management Meetings, and the Change System are DoIT tools and resources used for coordinating, monitoring, and controlling changes. The ISP has approved the use of these tools and resources when DoIT implements changes to ISP IT resources.

II. DEFINITIONS

II.A. Change – a modification, functional or performance enhancement, tuning, maintenance, development, installation, or removal of an ISP IT resource, including, but not limited to, applications and IT infrastructure.

II.A.1. Emergency change – an unscheduled change initiated on an urgent basis to correct a problem(s) that affects the delivery of service or to address something that cannot wait for the regular Change Management Meeting.

II.A.2. Major change – a high-risk, high-impact change that requires proper planning to prevent disruption in production environments. Examples: relocation of a data center or replacement of an enterprise solution.

II.A.3. Standard change – a medium-risk, medium-impact change that could have an effect on system established processes, procedures, or other systems reliant on these processes or data from the system being changed. Examples: significant operating system upgrades, changes to communication protocols, or changes to shared data.

II.B. Change Management Committee – a DoIT committee consisting of all Applications and Infrastructure Managers that meets on a weekly basis to assess/approve change requests. Members include a manager(s) from the Division of Justice Services (DJS) who has a broad scope of knowledge of systems that impact their area of responsibility.

II.C. Change Management Meeting – a weekly meeting of the Change Management Committee and personnel who submitted changes for the week or emergency changes for the prior week. There is also varying attendance from other technical personnel.

II.D. Change Request Form – a formal, documented request for a change to a system or data processing resource.

II.E. Change System – a database used to submit and record all change requests, their status, and associated details.

II.F. IT Environments:

II.F.1. Development – a software development space where developers can create and iterate software freely and without the risk of impacting users.

II.F.2. Production – a live environment, also known as deployment environment, where users can freely interact with the software.

II.F.3. Test – an environment used to put software through extensive testing to ensure it works as designed and detect flaws and vulnerabilities ensuring the software performs to expected standards before releasing.

II.G. Mission-Critical Applications or Infrastructure – any IT application or infrastructure required by ISP to respond and handle emergencies, calls for service, or to protect the safety of our officers and the general public.

II.H. User Acceptance Testing (UAT) – the process used to identify and correct defects and verify expectations, completeness, and quality of work. Various methods and levels of formality are employed depending on the nature of the change.

III. RESPONSIBILTIES

III.A. The ISP is responsible for:

III.A.1. Initiating the process for DoIT or another appropriate vendor to complete a Change Request Form.

III.A.2. Providing end users to perform UAT at various levels when needed.

III.A.3. Providing final approval for all application and infrastructure changes.

III.A.4. Ensuring all contracts with other IT vendors for computer systems or applications not maintained by DoIT have a change management process that meets or exceeds the standards outlined above. ISP management overseeing the IT project will ensure changes made are documented and approved prior to implementation, including, but not limited to, adequate segregation of duties to ensure strong internal controls are maintained.

III.B. Pursuant to the current Intergovernmental Agreement (IGA) between DoIT and the ISP, DoIT has accepted responsibility for:

III.B.1. Ensuring its current policies and procedures establish requirements for the handling of changes to IT resources that ensure an acceptable balance of risk and resource effectiveness and reduce the risk of potential disruption in services.

III.B.2. Utilizing Change Request Forms, conducting Change Management Meetings, and maintaining the Change System.

IV. PROCEDURES

IV.A. Submitting a Change Request

IV.A.1. Whenever a work unit within the ISP needs a change to an ISP controlled IT resource, the work unit must seek the approval of the appropriate Deputy Director and submit a proposed change to the DJS Deputy Director's Office for review and approval.

IV.A.2. The DJS Deputy Director's Office will submit the Change Request Form and a recommendation for review and approval by the Director or their designee.

IV.A.3. Once approved, the DJS Deputy Director's Office will notify the appropriate division to initiate the process for the change requests to DoIT. The Division will use DoIT's SharePoint link to complete a Change Request Form within the Change System and include any required information or documentation.

IV.A.4. DoIT will notify by email the Division that submitted the change request once the change is ready for UAT.

IV.B. Major changes require evaluation for determining the approval workflow and schedule.

IV.B.1. Major changes require active management and the Change Management Committee's approval.

IV.B.2. If applicable, the change request shall include comprehensive cost benefit, risk impact and financial impact analyses.

IV.B.3. Major changes should be developed, tested extensively, communicated, and trained. Major changes must be announced 90 calendar-days prior to implementation.

IV.C. Standard changes require active management and the Change Management Committee's approval and must be announced 30 calendar-days prior to implementation.

IV.D. Emergency changes are permitted to restore or minimize immediate operational impact(s) to mission critical infrastructure or applications.

IV.D.1. An emergency change is approved by the application manager and then reviewed at the next scheduled Change Management Meeting.

IV.D.2. Changes must be documented on a Change Request Form within the Change System.

IV.E. UAT Testing

IV.E.1. The ISP will provide end users to perform UAT testing when needed.

IV.E.2. All changes to applications and infrastructure will be tested before pushing it to production to minimize any errors once the change goes live. DoIT will provide ISP end users a testing document to memorialize the tests performed and the results. All testing forms will be maintained by DoIT and uploaded to the Change Request System.

IV.E.3. After the final approval via the Change Request Form is received from the ISP, the change may be pushed to production by DoIT.

IV.F. New System Development

IV.F.1. New system development will adhere to this policy to the extent that the new development may impact any other ISP controlled IT resource.

IV.F.2. Changes in scope for a specific development project, which will be tracked and managed by DoIT, will be communicated to the ISP pursuant to the current IGA.

-End of Directive-