ILLINOIS STATE POLICE DIRECTIVE
OPS-100, CONTINUITY OF OPERATIONS

RESCINDS:	**REVISED:**
OPS-100, 2023-176, revised 12-04-2023	09-23-2024 **2024-033**
RELATED DOCUMENTS:	**RELATED CALEA STANDARDS (6th Edition):**
ISP Continuity of Operations (COOP) Plan	46.1.1, 46.1.2, 46.1.5, 46.1.9, 46.1.13

I. POLICY

I.A. The Illinois State Police (ISP) will develop protocols and maintain a Continuity of Operations (COOP) Plan to ensure continuation of essential functions under all threats and conditions.

I.A.1. The COOP Plan will identify agency critical functions including, but not limited to: mission essential functions, orders of succession and delegations of authority, alternate facilities and communications, human capital allocation and vital record retention, etc. and provide a pre-planned response protocol in accordance with accepted best practices.

I.A.2. The COOP Plan shall be designated and maintained as sensitive and confidential documents.

I.B. The ISP is a client agency of the Department of Innovation and Technology (DoIT). In providing services and resources to its client agencies, DoIT operates a robust framework of information technology (IT) security policies including, but not limited to, contingency planning policy, which is adopted herein by reference.

I.B.1. The ISP adopts these policies, as well as the Intergovernmental Agreement (IGA) and Management Control Agreement (MCA) with DoIT, by reference.

I.B.2. The ISP is responsible for exerting management control as is currently documented in the IGA and MCA, especially as it pertains to its Criminal Justice Information Services (CJIS) systems and the data contained therein; and

I.B.3. DoIT shall adhere to these policies, the IGA and MCA, in providing services to the ISP.

I.C. The State of Illinois adopts the FBI's CJIS Security Policy as its minimum-security requirement for criminal justice information. All information systems developed, acquired, or utilized as a service by DoIT and/or its Client Agencies containing CJIS regulated information will incorporate this security standard. Entities may develop local security policies; however, the CJIS Security Policy shall be the minimum applicable standard, and local policy shall not detract from this baseline.

II. AUTHORITY

II.A. Illinois Emergency Operations Plan, Annex 2 - Continuity of Operations, Illinois Emergency Management Agency, October 2021

II.B. National Continuity Policy Implementation Plan, Homeland Security Council, August 2007

II.C. National Institute of Standards and Technology

II.D. National Security Presidential Directive 51/Homeland Security Presidential Directive 20, May 4, 2007

III. DEFINITIONS

III.A. Continuity of Operations (COOP) Plan – a COOP Plan, as defined in the National Continuity Policy Implementation Plan and the National Security Presidential Directive 51/Homeland Security Presidential Directive 20, is a document created in an effort to ensure that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents and technological or attack-related emergencies. The COOP Plan is developed through internal processes to ensure the capability exists to continue essential functions and services in response to a comprehensive array of potential emergencies or disasters.

III.B. Disaster Recovery Plan – a written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. The detailed document outlines how the ISP and our contracted vendors will respond effectively to an unplanned incident and resume business operations. Types of disasters include power outages, ransomware and malware attacks, natural disasters, etc.

III.C. System-level information – system-state information, operating systems and application software, and licenses.

III.D. User-level information – data generated by information system and/or application users.

IV. RESPONSIBILITIES

IV.A. The Chief of the ISP Office of Strategic Planning (OSP), Office of the Director (OOD), will:

IV.A.1. Maintain the ISP COOP Plans.

IV.A.1.a. All COOP Plans will be reviewed annually.
IV.A.1.b. Specific personnel information will be updated quarterly.
IV.A.1.c. The specific requirements for updating and reviewing COOP Plans will be identified in the Primary COOP Plan. The requirements will at a minimum include:

IV.A.1.c.1) Positions responsible for reviewing all COOP Plans.
IV.A.1.c.2) A schedule for COOP Plan reviews.

IV.A.2. Develop and conduct table-top and/or full-scale exercises to test the COOP Plans annually.

IV.A.3. Assist the Division of the Academy and Training (DAT) with the development of training related to COOP Plans.

IV.B. Unit Commanders will ensure that personnel under their command have completed assigned training related to COOP Plans.

IV.C. The Deputy Director of the Division of Justice Services (DJS) is responsible for ensuring user-level and system-level information are backed up daily, retained for at least 30 days, and are encrypted consistent with applicable CJIS Standards.

V. PROCEDURES

The ISP COOP Plan will:

V.A. Address the following elements:

V.A.1. Mission Essential Functions;

V.A.2. Orders of succession;

V.A.3. Delegations of authority;

V.A.4. Essential positions;

V.A.5. Backups of essential information technology systems, databases, and servers;

V.A.6. Continuity of facilities and resources;

V.A.7. Continuity of communications;

V.A.8. Essential records;

V.A.9. Tests, training, and exercises;

V.A.10. Disaster recovery and reconstitution.

V.B. Consist of:

V.B.1. A primary plan containing the above elements with generalized department-wide concepts of operations.

V.B.2. Annex plans that are ISP Division-specific.

VI. IT Systems Contingency Planning

VI.A. The ISP will work with DoIT to ensure IT systems contingency plans comply with the guidance of the National Institute of Standards and Technology. Deputy Directors will ensure supervisory personnel are appropriately trained regarding IT contingency plans.

VI.B. To maximize the effectiveness of contingency operations, each division will work with their IT vendors to ensure:

VI.B.1. Production databases, production application servers, and production file servers are backed up at least daily and retained for a period of at least 30 days.

VI.B.2. All disaster recovery plans within their authority outline the following components at a minimum:

VI.B.2.a. Backups of user-level information contained in operational systems for essential business functions;
VI.B.2.b. Backups of system-level information contained in the system;
VI.B.2.c. Backups of system documentation, including security- and privacy-related documentation;
VI.B.2.d. Encryption to protect the confidentiality, integrity, and availability of backup information;
VI.B.2.e. Testing backup information to verify media reliability and information integrity;
VI.B.2.f. Backup logs which are documented and reviewed regularly to verify data is accessible;
VI.B.2.g. Cryptographic mechanisms to prevent unauthorized disclosure and modification of CJI;
VI.B.2.h. Outage assessment procedures;
VI.B.2.i. A sequence for recovery activities;
VI.B.2.j. A plan for the reconstitution of the system to a previous version after a disruption, compromise, or failure; and
VI.B.2.k. A plan for post-recovery and reconstitution analysis.

NOTE: DJS will act as the point of contact for all IT contracts handled by DoIT assuming these responsibilities regardless of which divisions utilize the contract.

Indicates new or revised items.

-End of Directive-