ILLINOIS STATE POLICE DIRECTIVE
OPS-100, CONTINUITY OF OPERATIONS

RESCINDS:	**REVISED:**
OPS-100, 2022-185, revised 06-24-2022	12-04-2023 **2023-176**
RELATED DOCUMENTS:	**RELATED CALEA STANDARDS (6th Edition):**
	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 polices 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 Security Presidential Directive 51/Homeland Security Presidential Directive 20, May 4, 2007

III. DEFINITIONS

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.

IV. RESPONSIBILITIES

IV.A. The Chief of the ISP Office of Strategic Planning, Office of the Director, 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.

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. Essential Information Technology Systems;

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. 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. Information Systems Contingency Planning

The ISP will work with DoIT to ensure Information Technology 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.

Indicates new or revised items.

-End of Directive-