ILLINOIS STATE POLICE DIRECTIVE
SRV-221, INTERNET USE

RESCINDS: SRV-221, 2022-116 revised 03-09-2022.	**REVISED:** 01-25-2023 **2023-140**
RELATED DOCUMENTS: PER-030, ROC-002, SRV-201, SRV-204, SRV-208, SRV-209, SRV-218, SRV-222.	**RELATED CALEA STANDARDS (6th Edition):** 11.4.4, 54.1.1

I. POLICY

I.A. The Illinois State Police (ISP) will allow and encourage the use of Internet services to support the various missions of the Department.

II. DEFINITIONS

II.A. Anti-virus software - A program that detects malicious code within a program or electronic mail.

II.B. Home page - the main page of a website. The home page serves as an index or table of contents.

II.C. Internet - a global web connecting computers. Unlike online services, which are centrally controlled, the Internet is decentralized.

II.D. Website - a location on the World Wide Web.

II.E. World Wide Web - a system of Internet Servers that supports specially formatted documents.

III. PROCEDURES

III.A. Use of ISP's Internet service is limited to state business.

III.A.1. Supervisors can request and be granted permission from the First Deputy Director to review Internet use if the supervisor suspects unauthorized use or if an employee is under investigation.

III.A.2. ISP's Internet service must not be used to (the below conditions may be waived when part of an investigation and prior approval from a supervisor is obtained):

III.A.2.a. Communicate information that is illegal or unrelated to ISP's mission.
III.A.2.b. Access chat rooms or instant messaging unless doing so is required as part of a departmental investigation.
III.A.2.c. Disrupt or in any way detract from the effective operation and management of the workplace
III.A.2.d. Receive or transmit:

III.A.2.d.1) Any materials in violation of any government laws
III.A.2.d.2) Pornographic, obscene, abusive, or objectionable language or images in either public or private messages
III.A.2.d.3) Chain letters or broadcast messages

III.A.2.e. Gamble
III.A.2.f. Operate or promote a:

III.A.2.f.1) For-profit activity
III.A.2.f.2) Private business

III.A.2.g. Cause congestion of the network or otherwise interfere with the work of others such as streaming audio and streaming video, unless part of official duties

III.A.3. Internet e-mail accessed from ISP devices is not considered confidential and may in some instances be used as evidence in court cases.

III.A.4. ISP reserves the right to examine the content of the hard drive and any other component of any state-owned computer to inspect for unauthorized software and to examine e-mail and data for unauthorized use. Except to the extent required by law and as may be specified by ISP policy, there is no expectation of privacy for information maintained by or transmitted through state-owned computers.

III.B. Since the Internet does not conform with the security standards established for the state's protected information resources, sensitive or confidential information must not be allowed to flow unprotected through the Internet environment.

III.C. Each individual using the Internet must do so responsibly and professionally.

III.C.1. Incidental use, such as accessing weather information, reviewing news updates, or checking personal e-mail is permissible but only to the extent it does not disrupt the employee's regular duties and is authorized by the work location supervisor.

| III.C.2. Users that encounter illegal activities via the Internet must immediately report such activities to their supervisor and to the Department of Innovation and Technology (DoIT).

| III.D. Personnel found violating the provisions of this directive may face discipline up to, and including, termination in accordance with ISP Directives, PER-030, "Complaint and Disciplinary Investigations," PER-103, "Code Employee Disciplinary Rules," and ROC-002, "Rules of Conduct."

III.E. Supervisors will ensure all ISP Internet users are aware of the Department's data security policies and procedures.

III.F. Supervisors will review Internet use procedures and user responsibilities with new users as part of user training.

| III.G. All employees and contractual personnel share the responsibility for the security and integrity of ISP resources. Users should check the status of "Windows Security" on their ISP computers to ensure that no actions are needed by left clicking on the Windows Security Icon in the lower right of their computer screen and opening Virus & threat protection.

| III.H. Users are required to immediately report any virus or suspected virus to their supervisor, who will notify DoIT.

| III.I. Security Administration will notify users of known viruses and recommend preventative measures.

| III.J. Security Administration will assist users in the removal of a virus from infected microcomputers.

IV. RULES AND RESPONSIBILITIES

IV.A. Use of the Internet requires responsible judgment, supervisory discretion, and compliance with applicable laws and regulations. Users must be aware of information technology security and other privacy concerns.

IV.B. No person using the Internet via an ISP connection has any proprietary interest or expectation of privacy in the use of the Internet.

IV.C. All persons using ISP's connection to the Internet are subject to having their use monitored by the ISP at any time and without notice.

| Indicates new or revised items.

-End of Directive-