ILLINOIS STATE POLICE DIRECTIVE
SRV-201, USE OF ILLINOIS STATE POLICE COMPUTING EQUIPMENT AND RESOURCES

RESCINDS: SRV-201, 2009-047, revised 03-05-2009.	**REVISED:** 10-24-2017 **0217-081**
RELATED DOCUMENTS: SRV-200, SRV-204, SRV-206, SRV-211, SRV-218, SRV-220, SRV-221	**RELATED CALEA STANDARDS:** 11.4.4, 82.1.6, 82.1.7

I. POLICY

The Illinois State Police (ISP) will ensure ISP equipment and computing resources are used for conducting ISP or State of Illinois business.

II. DEFINITIONS

II.A. Authorized program - a program approved by supervisory personnel for use in the Department.

II.B. ISP security directives - those directives that regulate access to and use of ISP computing resources. They are:

II.B.1. SRV-200, “Information Security and Disposal of Personal Information”

II.B.2. SRV-201, “Use of Illinois State Police Computing Equipment and Resources”

II.B.3. SRV-204, “Local Area Network (LAN) and Wide Area Network (WAN) Access and Administration”

II.B.4. SRV-206, “Use of E-Mail”

II.B.5. SRV-208, “Mobile Data Computer Systems”

II.B.6. SRV-211, “Investigative Indices System”

II.B.7. SRV-214, “Computer Aided Dispatch (CAD) and Traffic Information and Planning Systems (TIPS) Data Access and Dissemination”

II.B.8. SRV-215, “Field Notification Program”

II.B.9. SRV-217, “Law Enforcement Agencies Data System (LEADS) Help Program”

II.B.10. SRV-218, “Computer Password Control”

II.B.11. SRV-220, “Virus Security”

II.B.12. SRV-221, “Internet Use”

II.B.13. SRV-222, “Social Networking/Media Guidelines”

II.B.14. SRV-223, “Access to Criminal Justice Information”

II.C. Social networking websites – any computer network sites that focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Examples of social networking websites include but are not limited to: Facebook, MySpace, LinkedIn, Twitter, Google+ and sites that allow users to post personal blogs.

II.D. Supervisor - an individual that is responsible for personnel within a work unit.

II.E. User - any person who accesses any ISP computing resource.

III. PROCEDURES

III.A. All programs developed on ISP computing resources become the property of the ISP.

III.B. Employees can use computing resources when approved by their immediate supervisor to help complete the requirements of educational courses.

III.C. Users will:

III.C.1. Virus-check all software and data files prior to installing software programs or data files on ISP hardware. During the investigation of computer-related crimes by certified ISP computer examiners, where it is not feasible to check software and data files prior to installation, the user will assure, when practicable, anti-virus software is running during installation.

III.C.2. Only install authorized programs, data files, and software on ISP computers. The user's supervisor must approve any exceptions necessary for conducting official ISP business.

III.C.3. Use computing resources for official state business only.

III.C.4. Ensure they do not disclose or allow others to use their individual passwords (see ISP Directive SRV-218, "Computer Password Control").

III.C.5. Report any unauthorized use of information, data, or computing resources to their supervisor.

III.C.6. Read and comply with all ISP security directives applicable to their work assignment prior to initial access to ISP computing resources.

III.D. Supervisors will instruct personnel within their work unit and personnel transferring into their work unit to read ISP security directives applicable to their work unit.

III.E. Users will **not** use ISP computing resources for:

III.E.1. Developing programs or electronic communication for non-state of Illinois business.

III.E.2. Playing games, other than those associated with training or educational purposes and approved by an immediate supervisor.

III.E.3. Accessing and using:

III.E.3.a. Pornographic sites unless required by job responsibility or duties.
III.E.3.b. Entertainment related Internet sites, which include but are not limited to streaming video, streaming audio, or other technologies for personal use.
III.E.3.c. For purchase or sales, online auction, classified sites, or other e-commerce sites.
III.E.3.d. Social networking websites unless required by job responsibility or duties.

III.E.4. Circulating any malicious or derogatory information, or publicly criticizing or ridiculing the Department or its employees.

III.F. 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 Employees Disciplinary Rules," and ROC-002, "Rules of Conduct."

Indicates new or revised items.

-End of Directive-