ILLINOIS STATE POLICE DIRECTIVE
SRV-206, USE OF E-MAIL

RESCINDS: SRV-206, 2013-068, revised 10-11-2013.	**REVISED:** 01-14-2016 **2016-003**
RELATED DOCUMENTS: SRV-218	**RELATED CALEA STANDARDS:** 82.1.1, 82.1.6

I. POLICY

The Illinois State Police (ISP) will make an electronic message system (e-mail) available to ISP and contractual personnel during their course of employment.

NOTE: The ISP has the right to read any e-mail sent/received via the Department's e-mail system. Employees should be aware of the fact they have no expectation of privacy regarding the use of e-mail.

II. DEFINITIONS

II.A. E-mail - a means of communication using commonly accepted e-mail software and protocols that electronically convey information, including text and attachments, from one person to one or many persons. For the purpose of this directive, e-mail does not include other forms of electronic communications such as Illinois Wireless Information Network (IWIN) Messaging and National Law Enforcement Telecommunications System (NLETS)/Law Enforcement Agencies Data System (LEADS) Administrative Messages that are addressed in other ISP directives.

II.B. Internet - the collection of inter-connected networks that use Transmission Control Protocol/Internet Protocol (TCP/IP).

II.C. Intranet - the collection of ISP internal inter-connected networks that use TCP/IP protocols.

II.D. Lotus Notes - the electronic message platform currently sanctioned and supported by the ISP.

II.E. Lotus Notes Administration - a unit within the Information Services Bureau (ISB), Division of Administration (DOA) assigned the responsibility of overseeing Lotus Notes computing resources.

II.F. Owner - the owner of a collection of information in the Division/Bureau responsible for the business results of an application, system, or the business use of this information. Ownership of applications or systems may be shared by data-owners of different organizational units.

II.G. Personal computer - a stand-alone or networked computer equipped with system, utility, application software, input/output devices, and other peripherals that an individual needs to perform one or more tasks.

II.H. Security Administration - a unit within ISB designated to assign control access to ISP computing resources.

II.I. TCP/IP - a common language that computers on the internet use for communications.

II.J. User - any person who has been authorized to read, enter, update, or disseminate information by the owner of the system or application data.

III. PROCEDURES

III.A. Security Administration:

III.A.1. Reviews and approves or disapproves access to Lotus Notes.

III.A.2. Assigns the Resource Access Control Facility (RACF) user identification (ID) associated with a Lotus Notes user ID to allow access to Lotus Notes via the Intranet or Internet and deletes user IDs after 180 days of inactivity.

III.A.3. Receives notification of changes in an employee's status such as separation, leave of absence, or suspension from the supervisor, Wage Electronic Notification, or LEADS directed messages; makes the necessary changes to the user's RACF authorization; and notifies the Lotus Notes Administration of changes in an employee's status.

III.B. Lotus Notes Administration:

III.B.1. Assigns the Lotus Notes user ID after receiving a request from the user's supervisor, the site coordinator, or Security Administration.

III.B.2. Receives system notifications from Security Administration of changes in status of personnel employed by ISP.

III.B.3. Reviews Lotus Notes system logs for errors, mail waiting to be sent, and security violations and notifies appropriate management of security violations.

III.B.4. Audits system access semi-annually for users who have not accessed their Lotus Notes system and notifies supervisors of personnel who are not accessing Lotus Notes and deletes users from Lotus Notes after 180 days of inactivity.

III.B.5. Removes users from Lotus Notes upon notification from Security Administration that a user's employment with the ISP has been terminated.

III.C. Supervisors will:

III.C.1. Encourage the use of electronic messaging and calendar systems for appropriate staff who have been authorized e-mail access.

III.C.2. Ensure employees have read and are familiar with e-mail policies.

III.C.3. Take appropriate disciplinary action if abuse of e-mail use as detailed in paragraph III.G. is discovered.

III.C.4. Ensure their employees fill out Company, Work Phone Number, Work Location, Manager, and state-owned cell phone number (when applicable) fields in the Notes Address Book.

III.C.5. Ensure their employees use the Lotus Notes Signature function for all e-mail messages as detailed in paragraph III.D.9.

III.D. Users will:

III.D.1. Access and monitor their Lotus Notes messages and calendar on a daily basis during their normal work hours.

III.D.2. Use Lotus Notes message system equipment in an authorized, safe, and legitimate manner.

III.D.3. Monitor their Lotus Notes files and retain and purge the files, as appropriate, in compliance with ADM-137, "Records Retention/Destruction Schedules" and the Illinois State Records Act, 5 ILCS 160/1, et seq.

III.D.4. Change their Lotus Notes password monthly.

III.D.5. Change their RACF password monthly.

III.D.6. Be encouraged to use the Out of Office function when they are out of the office for training, vacation, leaves, etc. The user should contact the ISP Help Desk at 1-866-532-3700 or 1-217-782-4155 for assistance with setting the Out of Office function.

III.D.7. Be encouraged to designate an e-mail delegate when appropriate.

III.D.8. Ensure they fill out Company, Work Phone Number, Work Location, Manager, and state-owned cell phone number (when applicable) fields in the Notes Address Book. Sworn officers will include their home (land-line or cellular) telephone number in the Notes Address Book. Code employees are encouraged to include their home telephone number in the Notes Address Book.

III.D.9. Use the Lotus Notes Signature function for all e-mail messages. At a minimum, the user will include their name, rank (if applicable), work unit, and office phone number.

III.E. E-mail Delegates

III.E.1. Users are encouraged to assign a delegate for their e-mail to ensure the capability for messages being checked when out of the office for training, vacation, leaves, etc.

III.E.2. A delegate is required to take appropriate action for the user's e-mail for which they are delegates.

III.E.3. Users should contact the ISP HELPDESK at 1-866-532-3700 or 1-217-782-4155 for assistance with setting the delegate function.

III.F. Security procedures

III.F.1. Password protocols are to be followed by all users of ISP e-mail system. (See directive SRV-218, "Computer Password Control.")

III.F.2. E-mail sent to users via the Internet is **not** secure. Users must take appropriate action to ensure e-mail sent to non-ISP personnel is properly secured.

III.G. E-mail cannot be used for:

III.G.1. Harassment in any form

III.G.2. Copyright infringement

III.G.3. Excessive use for non-ISP business (limited use may occur only if it does not adversely affect the performance of official duties by the employee)

III.G.4. Violations of published ISP operating system security standards or procedures

III.G.5. Chain letters

III.G.6. Unauthorized release of information

III.G.7. Any unlawful activity

IV. RULES AND REGULATIONS

IV.A. E-mail is a tool provided by the ISP to enhance communications within the Department and with other entities outside of the ISP. Use of the ISP e-mail system for other than official state business should be held to a minimum. Employees found to have used the e-mail system excessively for personal business are subject to disciplinary action, including termination of employment.

IV.B. No person using ISP's e-mail system has any proprietary interest or expectation of privacy in the use of the e-mail system, including the content of information sent and/or received.

IV.C. ISB may establish guidelines on sending large file attachments and large distributions (e.g., LDALL).

IV.D. All persons using ISP's e-mail system are subject to having their usage monitored by ISP at any time and without notice, including the content of information sent and/or received.

Indicates new or revised items.

-End of Directive-