ILLINOIS STATE POLICE DIRECTIVE
SRV-225, PROCEDURES FOR THE REMOVAL OF INFORMATION AND DESTRUCTION OF PHYSICAL MEDIA

RESCINDS: SRV-225, 2022-117, revised 03-09-2022.	**REVISED:** 12-04-2023 **2023-181**
RELATED DOCUMENTS: PER-030, SRV-200, SRV-201, SRV-204, SRV-206, SRV-211, SRV-218, SRV-221	**RELATED CALEA STANDARDS (6th Edition):** 82.1.1, 82.1.6, 82.1.2, 82.1.3, 82.3.4, 82.3.5, 81.1.1, 84.1.5, 84.1.6, 84.1.7, 84.1.8

I. POLICY

I.A. The Illinois State Police (ISP) shall take all necessary steps to protect ISP Data from unauthorized disclosure by defining the requirements for permanently removing ISP Data from media before disposal or reuse, a process called "media sanitization," and properly disposing of media.

I.A.1. The reuse, recycling, or disposal of computers and other technologies that can store data pose a significant risk since data can easily be recovered with readily available tools, even data from files that were deleted long ago or a hard drive that was reformatted.

I.A.2. Failure to properly purge data in these circumstances may result in unauthorized access to ISP Data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

I.B. To prevent unauthorized disclosure of data:

I.B.1. Media leaving control of the ISP and destined for reuse or disposal must have all data purged in a manner that renders the data unrecoverable; and

I.B.2. Media that will be reused within the Department should likewise have all data purged to prevent unauthorized disclosure.

I.C. 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. These policies establish prescribed standards and operational requirements, for both DoIT and its client agencies, aimed at protecting the security, processing, integrity, availability, and confidentiality of State of Illinois systems and data.

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

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

I.D. 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. DEFINITIONS

II.A. Confidential Data - Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.

II.B. Data - Any data related to ISP functions that are stored on ISP information technology systems. This applies to any format or media (in other words, it is not limited to electronic data)

II.C. Degaussing - Demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.

II.D. Disintegration - A physically destructive method of sanitizing data; the act of separating into component parts.

II.E. Incineration - A physically destructive method of sanitizing media; the act of burning completely to ashes.

II.F. Media - Material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CDs and DVDs.

II.G. Media sanitization - The process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

II.H. Pulverization - A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

II.I. Purging - A media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

III. ROLES AND RESPONSIBILITIES

III.A. The Division of Justice Services (DJS) will make relevant DoIT policies available to its employees via the ISP intranet.

III.A.1. The DJS will review the ISP intranet annually no later than October 1 each year to ensure the most current policies are posted.

III.A.2. Each division is responsible for ensuring ISP employees are aware of current DoIT policies.

III.B. The Department of Innovation and Technology (DoIT) is responsible for ensuring that ISP data are properly removed or destroyed from media before it leaves the control of the ISP for reuse or disposal.

III.B.1. DoIT policy requires that shredding be performed by a CJIS certified technician.

III.B.2. An ISP witness shall be present when DoIT completes hard-drive shredding of ISP equipment.

IV. IMPLEMENTATION PROCEDURES

IV.A. While the primary purpose of this policy is to protect ISP data (e.g., data classified either internal or confidential), it is often very difficult to separate these classifications from public or personal data on the media or determine conclusively that remnants of non-public data are not recoverable. Therefore, it is often most expedient to purge all data from the media before reuse or disposal rather than try to selectively sanitize the sensitive data.

IV.B. Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. However, if physical destruction is contracted to a third party outside the ISP, data must be purged from the media before giving it to DoIT.

IV.C. Equipment images prior to sanitization

IV.C.1. All Bureau Chief positions and higher or Lieutenant and above will have the equipment imaged prior to sanitization. This image will be kept on a secure network volume if needed for legal or operational issues.

IV.C.2. All other equipment will have a copy of the user files backed up temporarily if the data files are to be transferred to another piece of equipment at the request of the supervisor.

V. SPECIFIC INSTRUCTIONS FOR DIFFERENT TYPES OF MEDIA AND REGULATIONS

V.A. Electronic Storage Media: (hard disk drives in computers, external hard drives, USB flash drives, magnetic tapes, solid state drives (SSD), etc.)

V.A.1. If purging is done by overwriting the data, the entire media/device must be overwritten with a minimum of three passes. SSD drives must be wiped/erased by an approved DoIT tool or program.

V.A.2. Equipment that can store data, such as desktop and laptop computers or external hard drives, and is permanently leaving the control of the ISP should have all data storage devices removed before disposition. If the equipment leaving ISP control must retain the data storage devices, all data must be properly purged.

V.A.3. The only acceptable methods for physically destroying a hard drive are shredding, pulverization, disintegration, or incineration.

V.A.4. Degaussing is an acceptable method of purging data from magnetic media.

V.B. Optical Media: (e.g., CDs and DVDs)

Optical media containing internal or confidential data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

V.C. Smartphones and other handheld devices

Mobile devices like Smartphones (e.g., Blackberry, Windows, or iPhone), stored information often contains personal or other sensitive information. Any data must be purged from these devices before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.

VI. DOCUMENTATION

The ISP will instruct DoIT to ensure appropriate documentation is retained to monitor and demonstrate compliance with the requirements of its IT security policies and procedures. The ISP will instruct DoIT to ensure appropriate quality assurance measures are implemented to confirm compliance on an annual basis.

Indicates new or revised items.

-End of Directive-