



|   |   |
|---|---|
| <b>CHAPTER # 26<br/>POLICE INFORMATION</b>  | <b>POLICY # 26.7<br/>DISCIPLINARY ACTIONS</b> |
| <p><i>This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only form the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline.</i></p> |   |
| Date Implemented: 11/18/2022  | Review Date:                                  |

## **DISCIPLINARY POLICY**

In support of the Indian Hills Police Department's mission of public service to its citizens, the Indian Hills Police Department provides the needed technological resources needed to personnel to access FBI CJIS systems and information in support of the agency's mission. All agency personnel, with access to FBI Criminal Justice Information (CJI) or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care, and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by the Indian Hills Police Department's state CSO, and the FBI. To maintain the integrity and security of the Indian Hills Police Department's and FBI's CJIS systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations and contractual obligations. All existing laws and Indian Hills Police Department regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of the Indian Hills Police Department's computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

### ***Examples of Misuse with access to FBI CJI***

1. Using someone else's login that you are not the owner.
2. Leaving computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access Indian Hills Police Department systems and/or FBI CJIS systems and data in your name.
3. Allowing unauthorized person to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.
4. Allowing remote access of Indian Hills Police Department issued computer equipment to FBI CJIS systems and/or data without prior authorization by the Indian Hills Police Department.
5. Obtaining a computer account that you are not authorized to use.
6. Obtaining a password for a computer account of another account owner.
7. Using the Indian Hills Police Department network to gain unauthorized access to FBI CJI.
8. Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems.
9. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.
10. Violating terms of software and / or operating system licensing agreements or copyright laws.
11. Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in the Indian Hills Police Department for home use or for any customer or contractor.
12. Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with *Sample Agency* network performance.
13. Using electronic mail or instant messaging to harass others.
14. Masking the identity of an account or machine.
15. Posting materials publicly that violate existing laws or Indian Hills Police Department codes of conduct.
16. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner.
17. Using Indian Hills Police Department's technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or using official capacity.
18. Unauthorized possession of, loss of, or damage to Indian Hills Police Department's technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.
19. Maintaining FBI CJI or duplicate copies of official Indian Hills Police Department files in either manual or electronic formats at his or her place of residence or in other physically non--secure locations without express permission.
20. Using Indian Hills Police Department's technology resources and/or FBI CJIS systems for personal or financial gain.

21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.

22. Using personally owned devices on Indian Hills Police Department's network to include personally-owned thumb drives, CDs, mobile devices, tablets on Wi-Fi, etc. Personally-owned devices should not store Indian Hills Police Department data, State data, or FBI CJI.

The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by the Indian Hills Police Department on a case-by-case basis. Activities will not be considered misuse when authorized by appropriate Indian Hills Police Department officials for security or performance testing.

***Privacy Policy***

All agency personnel utilizing agency-issued technology resources funded by the Indian Hills Police Department expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of Indian Hills Police Department systems indicates consent to monitoring and recording. The Indian Hills Police Department reserves the right to access and audit all communications including electronic and physical media at rest, in transit and at end of life. Indian Hills Police Department personnel shall not store personal information with an expectation of personal privacy that are under the control and management of the Indian Hills Police Department.

***Personal Use of Agency Technology***

The computers, electronic media and services provided by the Indian Hills Police Department are primarily for business use to assist personnel in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

***Misuse Notification***

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, the Indian Hills Police Department shall: (i) establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.

All Indian Hills Police Department personnel are responsible to report misuse of Indian Hills Police Department technology resources to appropriate Indian Hills Police Department officials.

Local contact---LASO: [spratt@ihpd.org](mailto:spratt@ihpd.org) Phone: 502-338-4788

State contact---CSA ISO: Erin Marie Oliver [erin.oliver@ky.gov](mailto:erin.oliver@ky.gov) Phone: 502-382-6780

I have read the policy and rules above and I will abide the Indian Hills Police Department Disciplinary policy.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_/\_\_\_\_/20\_\_\_\_