Disciplinary Policy Sample

(Required Written Policy)

1.0 Purpose:

In support of *[agency name]*'s mission of public service to the city of/county of *[city or county name]* citizens, the *[agency name]* provides the needed technological resources needed to personnel to access MI/FBI CJIS systems and information in support of the agency's mission.

2.0 Scope

All agency personnel, with access to MI/FBI Criminal Justice Information (CJI) or any system with stored MI/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 MI/FBI CJIS is a privilege allowed by *[agency name]*, MI CSO, and the FBI. To maintain the integrity and security of the *[agency name]*'s and MI/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 *[agency name]* 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.

3.0 Policy

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 *[agency name]*'s computing and network resources and MI/FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

4.0 Examples of Misuse with access to MI/FBI CJI

1. Using someone else's login.
2. Leaving computer logged in with your login credentials unlocked, allowing anyone to access *[agency name]* systems and/or MI/FBI CJIS systems and data in your name.
3. Allowing unauthorized person to access MI/FBI CJI at any time for any reason. Note: Unauthorized use of the MI/FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.
4. Allowing remote access of *[agency name]* issued computer equipment to MI/FBI CJIS systems and/or data without prior authorization by *[agency name]*.
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 *[agency name]*'s network to gain unauthorized access to CJI.
8. Knowingly performing an act which will interfere with the normal operation of MI/FBI CJIS systems.
9. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to MI/FBI CJIS systems.
10. Masking the identity of an account or machine.
11. Posting materials publicly that violate existing laws.
12. 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.
13. Unauthorized possession of, loss of, or damage to *[agency name]*'s technology equipment with access to CJI through unreasonable carelessness or maliciousness.

14. Maintaining CJI or duplicate copies of official *[agency name]* files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.
15. Using *[agency name]*'s technology resources and/or CJIS systems for personal or financial gain.
16. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.
17. Using personally owned devices on *[agency name]*'s network to include personally-owned thumb drives, CDs, mobile devices, tablets on Wi Fi, etc. Personally owned devices should not store *[agency name]* data, or CJI.

The above listing is not all-inclusive and any suspected technology resource or MI/FBI CJIS system or MI/FBI CJI misuse will be handled by [*agency name]* on a case by case basis. Activities will not be considered misuse when authorized by appropriate [*agency name]* officials for security or performance testing.

5.0 Privacy Policy

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

6.0 Personal Use of Agency Technology

The computers, electronic media and services provided by *[agency name]* 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 system's use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

7.0 Misuse Notification

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, *[agency name]* shall: (i) establish an operational incident handling capability for all information systems with access to MI/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 *[agency name]* personnel are responsible to report misuse of *[agency name]* technology resources to appropriate *[agency name]* officials.

Local contact-LASO: firstnamelast@agencyname.com Phone:
State contact-CSA ISO: firstnamelast@state.gov Phone:

Other Related Resources:

- Notice of Criminal Penalties Document