I. Purpose

The purpose of this policy is to provide guidance for Maryland-National Capital Park Police (M-NCPP), Montgomery County Division agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. The Communications Section Supervisor will serve as the Terminal Agency Coordinator.

II. CJIS Account Access

A. No personally owned electronic devices are permitted to be used on Division computers with CJI access.

B. All accounts shall be reviewed at least every six months by the terminal agency coordinator Communications Section Supervisor or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain CJI. The Communications Section Supervisor may also conduct periodic reviews.

C. All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

D. The Communications Section Supervisor must disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated account administrator or assistant.)

E. The Communications Section Supervisor must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the Communications Section Supervisor will transfer the individual's account(s) to the new office (CJA).

F. The Communications Section Supervisor will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

G. Primary responsibility for account management belongs to the Communications Section Supervisor.

H. The Communications Section Supervisor shall:

1. Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
2. Periodically review existing accounts for validity (at least once every 6 months), and cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

III. Physical Protection

A. Communications, Investigative Services Section (ISS), and the Park Police Headquarters' (PPHQ) Server Room are secure locations. These locations will be secured with both, the physical and personnel security controls, sufficient to protect the FBI CJI and associated information systems. The perimeter of these rooms shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the PPHQ shall be identified with a sign at the entrance.

B. A visitor is defined as a person who visits the PPHQ on a temporary basis who is not employed by the Division and has no unescorted access to the physically secure location within the PPHQ where FBI CJI and associated information systems are located.

C. Visitors will:

1. Check in before entering a physically secure location by:
   a. Completing the visitor access log, which includes: name and visitor's agency, purpose for the visit, date of visit, time of arrival and departure, name and agency of person visited, and form of identification used to authenticate visitor.
   b. Visitor must provide a valid form of photo identification.
   c. Document badge number on visitor log if visitor badge issued. The visitor badge shall be worn on approved visitor's outer clothing and collected by the agency at the end of the visit.

2. Be accompanied by a Division escort at all times to include delivery or service personnel. An escort is defined as an authorized personnel who accompanies a visitor at all times while within Communications, ISS, or the PPHQ Server Room to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

3. Follow M-NCPP policy for authorized unescorted access.
   a. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the Division and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

b. Private contractors/vendors who require frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the M-NCPPC Police and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

4. Not be allowed to view screen information mitigating shoulder surfing.

5. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged by Division personnel. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified immediately.

6. Not be allowed to sponsor another visitor.

7. Not enter into a secure area with electronic devices unless approved by the Communications Section Supervisor to include cameras and mobile devices. Photographs are not allowed without permission of Division assigned personnel.

8. All requests by groups for tours of PPHQ will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.

D. Authorized Access- Only authorized personnel will have access to physically secure non-public locations. The Division will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent—and protect the agency from— physical, logical and electronic breaches.

E. All personnel with CJI physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJI access.
   a. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
   b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

c. Prior to granting access to CJI, the Division on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.
d. Refer to the CJIS Security Policy for handling cases of felony convictions, criminal records, arrest histories, etc.

2. Complete security awareness training.
   a. All authorized Division, Noncriminal Justice Agencies (NCJA) like ITI Division and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.
   b. Security awareness training will cover areas specified in the CJIS Security Policy at a minimum.

3. Be aware of who is in their secure area before accessing confidential data.
   a. Take appropriate action to protect all confidential data.
   b. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.

4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
   a. Report loss of issued keys, proximity cards, etc, to authorized agency personnel.
   b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the Officer in Charge to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.
   c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. (See below Disciplinary Policy.)

5. Properly protect from viruses, worms, Trojan horses, and other malicious code.

6. Web usage is for proper business purposes only.

7. Personally owned electronic devices are not permitted to be used on Division computers with CJI access.

8. Use of electronic media is allowed only by authorized Division personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

9. Division personnel will not e-mail CJI.

10. Report any physical security incidents to the Communications Section Supervisor to include facility access violations, loss of CJI, loss of laptops, cellphones thumb drives, CDs/DVDs, and printouts containing CJI.

11. Properly release hard copy printouts of CJI only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a "need to know" basis.

12. Ensure data centers with CJI are physically and logically secure.

13. Keep appropriate Division security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.

14. Not use food or drink around information technology equipment.

15. Only use marked alarmed fire exits in emergency situations.

16. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries.

F. Roles and Responsibilities:

1. Communications Section Supervisor - The Communications Section Supervisor serves as the point-of-contact at the Division for matters relating to CJIS information access. The Communications Section Supervisor administers CJIS systems programs within the agency and oversees the agency's compliance with FBI and state CJIS systems policies.
    a. Identify who is using the CSA (state) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
    b. Identify and document how the equipment is connected to the state system.
    c. Ensure that personnel security screening procedures are being followed as stated in this policy.
    d. Ensure the approved and appropriate security measures are in place and working as expected.
    e. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.
    f. Serve as the security point of contact (POC) to the FBI CJIS Division Information Security Officer (ISO).
    g. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
    h. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.

i. Identified as the POC on security-related issues for their respective agencies and shall ensure institute the CSA incident response reporting procedures are instituted at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

2. Information Technology Support - In coordination with above roles, all vetted IT support staff will protect CJI from compromise at the Division by performing the following:
   a. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted, and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the Division. For agencies who submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.
   b. Be knowledgeable of required M-NCPP technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit, and at the end of life.
   c. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.
   d. Properly protect the Division's CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).
   e. Install and update antivirus on computers, laptops, MDTs, servers, etc.
   f. Data backup and storage—centralized or decentralized approach.
   g. Perform data backups and take appropriate measures to protect all stored CJI.
   h. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured location.
   i. Ensure any media released from the M-NCPPC Police is properly sanitized/destroyed. (See Sanitization and Destruction Policy)
   j. Timely application of system patches—part of configuration management.
      1.) The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
   k. Access control measures
      1.) Address least privilege and separation of duties.
      2.) Enable event logging of:
         i. Successful and unsuccessful system log-on attempts.

ii. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
iii. Successful and unsuccessful attempts to change account passwords.
iv. Successful and unsuccessful actions by privileged accounts.
v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

3.) Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

l. Account Management in coordination with Communications Section Supervisor

1.) Agencies shall ensure that all user IDs belong to currently authorized users.
2.) Keep login access current, updated, and monitored. Remove or disable terminated, transferred, or associated accounts.
3.) Authenticate verified users as uniquely identified.
4.) Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
5.) Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
6.) Passwords
i. Be a minimum length of eight (8) characters on all systems.
ii. Not be a dictionary word or proper name.
iii. Not be the same as the User ID.
iv. Expire within a maximum of 90 calendar days.
v. Not be identical to the previous ten (10) passwords.
vi. Not be transmitted in the clear or plaintext outside the secure location.
vii. Not be displayed when entered.
viii. Ensure passwords are only reset for authorized user.

G. Network infrastructure protection measures.

1. Take action to protect CJI-related data from unauthorized public access.

2. Control access, monitor, enabling, and updating configurations of boundary protection firewalls.

3. Enable and update personal firewall on mobile devices as needed.

4. Ensure confidential electronic data is only transmitted on secure network channels using encryption and advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods.

5. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network.

6. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.

7. Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by the Police Division. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.

H. Communicate and keep the Division informed of all scheduled and unscheduled network and computer downtimes, all security incidents, and misuse. The ultimate information technology management control belongs to the Police Division.

I. Visitors to Secured Areas - Administration of the Visitor Check-In/Check-Out procedure is the responsibility of Communications personnel. Prior to visitor gaining access to physically secure area:

1. The visitor will be screened by the Division personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by the Chief, Park Police Division.

2. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by the Chief, Park Police Division.

3. Escort personnel will acknowledge being responsible for properly evacuating visitor in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures.

4. Escort and/or Front-Desk personnel will validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to Visitor departure.

5. All Division personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to the Communications Section Supervisor.

J. Penalties

1. Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution, and/or termination.

2. Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization, or prosecution in the case of criminal activity.

IV. Media Protections

A. The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

B. The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the Division. This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

C. Authorized Division personnel shall protect and control electronic and physical CJI while at rest and in transit. The Division will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the Communications Section Supervisor. Procedures shall be defined for securely handling, transporting, and storing media.

D. Media Storage and Access:

1. Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.

2. To protect CJI, Division personnel shall:
   a. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
   b. Restrict access to electronic and physical media to authorized individuals.
   c. Ensure that only authorized users remove printed form or digital media form CJI.

d. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques, and procedures.

e. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

f. Store all hardcopy CJI printouts maintained by the M-NCPPC Police in a secure area accessible to only those employees whose job function requires them to handle such documents.

g. Safeguard all CJI by the Division against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.

h. Take appropriate action when in possession of CJI while not in a secure area:

1.) CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.

2.) Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

3.) Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.

4.) Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of CJI.

E. Media Transport - Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

F. Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or

2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

G. The Division personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.

2. Restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.

H. The Division personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.

2. Limiting the collection, disclosure, sharing, and use of CJI.

3. Following the least privilege and role based rules for allowing access. Limit access to CJI to only those people or roles that require access.

4. Securing hand carried confidential electronic and paper documents by:
   a. Storing CJI in a locked briefcase or lockbox.
   b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
   c. For hard copy printouts or CJI documents:
      1.) Package hard copy printouts in such a way as to not have any CJI information viewable.
      2.) That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

5. Not taking CJI home or when traveling unless authorized by Communications Section Supervisor. When disposing of confidential documents, use a shredder.

I. Electronic Media Sanitization and Disposal - The agency shall sanitize, that is, overwrite at least three times prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (incinerated.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to "Sanitization Destruction Policy".

J. Breach Notification and Incident Reporting - The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

K. Roles and Responsibilities

1. If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:
   a. Division personnel shall notify his/her supervisor or the Communications Section Supervisor and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.
   b. The supervisor will communicate the situation to the Communications Section Supervisor to notify of the loss or disclosure of CJI records.
   c. The Communications Section Supervisor will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.

2. The CSA ISO will:
   a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
   b. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
   c. Act as a single POC for their jurisdictional area for requesting incident response assistance.

L. Penalties - Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution, and/or termination.

V. DISCIPLINARY POLICY

A. In support of the Maryland-National Capital Park Police, Montgomery County Division's mission of public service to Montgomery County of and its citizens, the Division provides the needed technological resources for 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 Division, state CSO, and the FBI. To maintain the integrity and security of the Division'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 M-NCPPC 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.

B. Misuse of computing, networking, or information resources may result in temporary or permanent restriction of computing privileges up to, and including, 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 M-NCPPC's computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

C. 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 Division's 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 Division's issued computer equipment to FBI CJIS systems and/or data without prior authorization by Division.

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 Division's 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 Division, for home use, or for any customer or contractor.

12. Deliberately wasting computing resources to include streaming audio or videos for personal use that interferes with Division 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 Division's 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 Division's technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.

18. Unauthorized possession of, loss of, or damage to Division's technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.

19. Maintaining FBI CJI or duplicate copies of official Division 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 Division'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 Division's network to include personally-owned thumb drives, CDs, mobile devices, tablets on WiFi, etc. Personally owned devices should not store Division's data, State data, or FBI CJI.

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

E. Privacy Policy - All agency personnel utilizing agency-issued technology resources funded by the Division expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of Division systems indicates consent to monitoring and recording. The Division 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. Division personnel shall not store personal information with an expectation of personal privacy that are under the control and management of Division.

F. Personal Use of Agency Technology - The computers, electronic media, and services provided by Division 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.

G. Misuse Notification

1. Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, Division 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.

2. 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.

3. All Division personnel are responsible to report misuse of M-NC Park Police technology resources to appropriate Division officials.

Local contact-Deborah.hagberg@mncparkpolice.org Phone:301-929-2713
State contact-CSAISO: ed.nabors@maryland.gov Phone:410-585-3175

Issuing Authority: _____ 3/30/16

Chief Antonio DeVaul
Maryland-National Capital Park Police
Montgomery County Division

End of Directive