1.1006 INFORMATION SYSTEMS SECURITY AND ACCEPTABLE USE

A. This policy defines the Information System Security responsibilities and acceptable use rights for employees, guests, vendors and contractors (hereinafter, "Users") of University of Maryland's Department of Public Safety ("UMDPS", or alternatively, the "Department") information system resources. Information systems include all platforms / operating systems, all computer sizes and equipment, and all applications and data (whether developed in-house or acquired from third parties) contained on those systems.
B. All individuals that are granted access to the UMDPS network and information systems including but not limited to full and part-time employees, temporary workers, contractors, and those employed by others to perform UMDPS work, are covered by this policy and shall comply with this and associated policies, procedures and guidelines.

1.1006.10 User Access Responsibilities

A. Employees will comply with The University of Maryland's "Guidelines for the Acceptable Use of Computing Resources" and "Using Software, A Guide to the Ethical and Legal Use of Software for Members of the Academic Community." Questions about those directives may be brought to the attention of the agency's Information Technology coordinator, the President's Legal Office, or the Coordinator of Policy and Ethics in the University's Academic Information Technical Services.
    1. All agency computers and computer systems are the property of the University of Maryland.
    2. All computer systems and information stored within the computer systems are also the property of the University of Maryland and may be monitored.
    3. Access to the computers and computer systems and the local area network is provided to authorized users only. Accounts issued to individuals are for the sole use of that individual and are non-transferable.
    4. Unauthorized access to the local area network, files, and/or computers is in violation of Maryland Criminal law 8-606 and 7-302 and may result in prosecution or disciplinary action.
B. All information and data processing systems to which users are given access are to be used only to conduct the activities authorized by the Department. The use of these resources must be conducted according to the policies, standards, and procedures instituted by the Department or on its behalf. The unauthorized use or disclosure of information provided by these data processing systems may constitute a violation of Department, State, and/or Federal laws which will result in disciplinary action consistent with the policies and procedures of the Department.
    1. UMDPS Bureaus may require additional agreements regarding the confidentiality of specific types of information; for example, law enforcement records, criminal case files, personnel records, financial records, etc. This policy may augment such Bureau policies, but is not intended to replace policies which remain in effect.
    2. Users given access to which they are not privileged or entitled are required to report the circumstances immediately to their supervisor. Supervisors are responsible for determining the User's appropriate access rights. Supervisors must notify the Information Systems Unit should they determine that access rights need to be modified.
C. General Use Guidelines
    1. Users should log off the network at the end of each day and should lock their computers or logout of secure applications when away from their desk/office.
    2. Users should store important files on the network drives where files are backed up daily.
    3. All individual user passwords must be kept confidential. Users should not share their passwords with other users.
    4. Users should change their passwords when required or as necessary.
    5. Computer systems shall only be used by the employee that is currently logged in, or signed on to it.

1.1006.20 Rights of Information Ownership

A. The Department and its Bureaus retain the rights of ownership to all Information Systems resources including hardware, software, functionality, data, and related documentation developed by the Department's information systems users on behalf of the Department. All Department Information
B. Systems resources remain the exclusive property of the University of Maryland and/or the Department, unless otherwise prescribed by other contractual agreements.

1.1006.30 Internal Network and Internet

A. The Internet is a world-wide collection of interconnected computer networks. The Department's local network, DRAGNET, is the UMDPS controlled network connected to the Internet.
B. While in performance of work-related functions, while on the job, or while using publicly owned or provided information processing resources, UMDPS users are expected to use the network and Internet responsibly and professionally. Users shall make no intentional use of these services in an illegal, malicious, or obscene manner.
C. Users may make reasonable personal use of publicly owned or provided DRAGNET or Internet resources as long as:
    1. The direct measurable cost to the public is none, is negligible, or access supports the mission of the agency
    2. There is no negative impact on user's performance of public duties;
    3. The policy is applied equitably among all personnel of the agency;
    4. Users may be required to reimburse the agency if costs are incurred that do not have prior approval by the Department or Bureau.
    5. When sending or forwarding e-mail via departmental e-mail accounts, Users shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden, unless otherwise allowed by law to make anonymous postings.
    6. Users are responsible for protecting UMDPS sensitive information by following the UMDPS policies and UMDPS Bureau policies and procedures.
D. Users have a responsibility to ensure, to the best of their ability, that all public information disseminated via DRAGNET and the Internet is accurate. Users shall provide in association with such information the date at which it was current and an e-mail address allowing the recipient to contact the public staff responsible for making the information available in its current form.
E. Users shall avoid unnecessary network traffic and interference with other users, including but not limited to:
    1. Subscribing to or otherwise authorizing the transmission of unsolicited commercial advertising (SPAM) by UMDPS Users. Such use is strictly forbidden.
    2. This prohibition shall not include Mailings to individuals or entities on a mailing list so long as the individual or entity voluntarily placed his/her name on the mailing list.
F. The use of computer resources, including e-mail, to conduct any activities already prohibited by University personnel or

other UMDPS policies (such as private/personal fund raising, profit-making, political activities, etc.) is prohibited, without written authorization from the University. Mass emailing by employees that do not pertain to Department business is prohibited.

G. Users shall not use the Internet, DRAGNET, or any State information system to allow the unauthorized dissemination of confidential information, or for any purpose that is not permitted by UMDPS policies or would compromise public safety or public health.

H. Users shall not stalk others; post, transmit, or originate any unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication or any communication where the message, or its transmission or distribution, would constitute a criminal offense, a civil liability, or violation of any applicable law.

I. Users shall not access or attempt to gain access to any computer account to which they are not authorized. They shall not access or attempt to access any portions of the DRAGNET networks to which they are not authorized. Users also shall not intercept or attempt to intercept data transmissions of any kind to which they are not authorized.

J. Users shall not install, download, attach or play audio/video accessories, CD's, DVD's, MP3, etc. except that equipment or media which is required in the performance of UMDPS business. The use of UMDPS provided computer equipment for personal entertainment purposes is prohibited.

1.1006.40 Workstation Security

A. Each employee should guard against the loss of data stored within the various computers and computer systems operated or accessed by UMDPS employees and other individuals.

B. The following requirements apply to office, home, or other remote access locations if utilized for UMDPS business:
   1. As appropriate, sensitive computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, or behind locked doors, especially outside working hours;
   2. Personal computers and computer terminals should not be left logged on when unattended or not in use.;
   3. Classified or sensitive information should not be printed on a printer located in public areas. However, in the event that public printers must be used to print sensitive or classified information, such information shall be cleared from printers immediately.
   4. Users should store important files on the network drives where files are backed up daily;
   5. All individual user passwords must be kept confidential. Users should not share their passwords with other users. Users should change their passwords when required or as necessary; and
   6. Computer systems shall only be used by the employee that is currently logged in, or signed on to it.

1.1006.50 Media Storage

A. Sensitive information stored on external media (e.g., CDs, USB Drives) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as sensitive information.

B. The use of removable storage devices or external devices (e.g., USB Flash Drives) shall be restricted to authorized personnel in order to safeguard and protect confidential data and information technology assets. Authorization for the use of removable storage devices must be granted by the user's supervisor in writing and specify the intended use of the device. The Bureau management shall maintain an inventory of all authorizations and use of removable storage devices. Any use must meet UMDPS Removable Media Security Policy.

C. Users shall request the use of Department owned storage devices. Bureaus shall strive to provide state owned-storage devices to staff and thereby limit the use of any personal device used to conduct any University business. Any use of personal devices must be disclosed to the supervisor and be approved.

D. Mobile computing devices and removable storage devices (e.g., laptops, PDAs, USB flash drives, etc) must never be left in unsecured areas and their use must meet UMDPS security standards. Any incidents of misuse, theft, or loss of data must be reported to the supervisor and to the Bureau Commander.

E. UMDPS sensitive or confidential information shall not be stored at home without appropriate authorization from the user's supervisor/manager, in consultation with the Bureau Commander. Users shall follow appropriate physical safeguards for offsite use. Documentation of authorization and storage of sensitive information in the home shall be maintained in accordance with the Bureau's procedures.

F. The UMPDS Information Systems Unit will control physical and digital access and securely stores information system media within a controlled area.

G. All storage attached, associated with, or extracted from UMDPS systems will be kept securely in the Information Systems Unit or submitted as evidence for secure safekeeping consistent with **2.506.10 Submitting Property/Evidence to Logistics.**

1.1006.51 Media Sanitization

A. The UMDPS Information Systems Unit will sanitize Information System media, both digital and non-digital, prior to internal reissue or disposal.

B. Disk storage devices that are ready for reissue or disposal will be scrubbed. They will be scrubbed (0s and 1s written in a random pattern) a minimum of three times before reissue or disposal. If a scrubbing program cannot be run, the disks contents will be noted an approval for destruction will be granted or denied by the UMDPS Information Technology Manager.

1.1006.52 Media Disposal

A. UMDPS Information Technology personnel will destroy storage media no longer needed or in a failed state once sanitized and approved by the UMPD Information Technology Manager.

B. When UMDPS storage media is no longer needed or in a failed state the disk will be kept securely on site until it is destroyed. Destruction will be coordinated with a company that can offer at least 10mm media shredding. Certification of destruction will be documented by serial number on a UMCP Certificate of Records Disposal form.

1.1006.53 Media Transport

A. Agency personnel protects and controls criminal justice data and restricts activities with transport of such media to authorized personnel. These personnel include, but are not limited to:
   1. Logistics Unit employees;
   2. Records Unit employees;
   3. Communications Unit employees; and/or
   4. Information Technology employees.

B. UMDPS will not transport agency criminal justice or information deemed sensitive outside of its secured facilities unless required for court proceedings or other law enforcement sensitive activities. If required for court, this information should be submitted for chain of custody purposes to the Logistics Unit consistent with **2.506.10 Submitting Property/Evidence to Logistics.**

1.1006.55 User Privacy

A. All users of the Department's information systems are advised that their use of these systems may be subject to monitoring and filtering.
   1. UMDPS reserves the right to monitor randomly and/or systematically the use of Internet and UMDPS information systems connections and traffic.
   2. Any activity conducted using the University and State's information systems (including but not limited to computers, Networks, e-mail, etc.) may be monitored, logged, recorded, filtered, archived, or used for any other purposes, pursuant to applicable Departmental policies and State and Federal laws or rules.
   3. The Department reserves the right to perform these actions with or without specific notice to the user.

1.1006.60 Software and Hardware

A. All software licenses purchased by the Department of Public Safety are the property of the Department of Public Safety.
   1. Software is not to be copied for personal use, except as permitted by software licensing agreements.
   2. Personal software is not allowed on University computers except in rare job-related instances.
   3. If you wish to install any software, you must obtain permission of the agency's Information Technology coordinator.

B. Installation of Software or Hardware
   1. UMDPS information system hardware and software installations and alterations are handled by authorized UMDPS Information System Unit employees, designated staff, or contractors only. Users shall not install new or make changes to existing information system hardware or software without prior authorization by the Information Systems Unit.
   2. Users shall not download software from the Internet unless specifically approved by the user's supervisor and the designated Information Systems Unit personnel. Downloading audio or video stream for a work related webinar or audio conference is permissible without prior authorization.

C. Purchasing Software and Hardware
   1. All purchases must be approved by the Information Systems manager and the employee's unit manager prior to purchase.
   2. Purchases made without the prior consent of the Information Systems manager will be subject to disciplinary action consistent with **2.900 Complaints & Discipline.**

1.1006.70 Computer Viruses: Malicious Code

A. It is the responsibility of each User to help prevent the introduction and spread of computer viruses and other malicious code. All personal computers in the Department must have the provided virus detection software running at all times.
   1. Users should immediately contact their manager or supervisor or Bureau Commander, and submit a Department IT Request for service when a virus is suspected or detected, so that it may be confirmed and removed by the appropriate Information Systems Unit personnel.
   2. Users must report all information security violations to the appropriate Department's Bureau Commander, who will notify the Information Systems Unit, who shall be responsible for notification of the Office of the Chief.

1.1006.80 Remote Access

A. Authorized users of UMDPS computer systems, networks and data repositories may be permitted to remotely connect to those systems, networks and data repositories to conduct Department-related business only.
   1. Users will only be granted remote access through secure, authenticated and managed access methods and in accordance with Information Systems Unit and UMDPS security policy and standards.
   2. Users shall not access agency networks via external connections from local or remote locations, including homes, hotel rooms, wireless devices, and off-site offices without knowledge of and compliance with the User Access Responsibilities section described above within this policy.

1.1006.90 Responsibilities of Information Systems Unit

A. Responsibilities of the Information Systems Unit include:
   1. Maintaining a liaison with Academic Information Technology Services (AITS) and other agencies to ensure off site server back-ups are conducted and maintained;
   2. Keeping the UMDPS computer systems running and configured properly;
   3. Coordinating purchasing, installing, training, operation, maintenance, storage, moving, and reconfiguration of UMDPS computers and computer hardware and software;
   4. Setting, modifying, and terminating individual and group computer security levels, access, permissions, and distribution access levels; and
   5. Conducting password audits at least annually.

B. The Information Systems unit is also responsible for creating access accounts for authorized users only.

1.1006.95 Managing System Access for Critical Systems (Requests for User Access)

A. Requests for User Access must be submitted via the UMDPS IT Request System. The supervisor, manager, or commander of the User must make the request and specify the appropriate role or level of access (view, edit, delete. full admin or specific application role).

B. The request for access will be assigned to the assigned application coordinator. The coordinator will review the request and either implement the request, deny the request, or modify the request with the appropriate access level or role. All actions will be documented within the original request.

C. The request for access will be document and maintained by UMDPS IT Personnel.

1.1006.96 Managing System Access for Critical Systems (Granting System Access)

A. Only UMDPS personnel responsible for establishing user accounts shall be able to grant system access.
Access rights must reflect employee status, job classification, or function and be granted based on the minimum access needed to perform their job duties (least privilege strategy).

B. Access shall be established in a manner such that every user is uniquely identifiable.

C. User access to system or shared accounts shall only be granted if absolutely necessary.
   1. Access to system or shared accounts shall be granted temporarily to users requiring the access to resolve issues with the system or perform updates.
   2. Individual user actions performed with the system or shared account must be identifiable and auditable.

D. Privileged access, such as that which allows users to perform administrative, programming, processing/authorization of business transactions, and security administration, must be segregated. If this is not feasible, additional security controls

must be put in place to mitigate risks. Examples of mitigating controls may include but are not limited to utilizing unique user IDs for every system user and logging all actions of each user.

E. Proper authorizations must exist and be documented for each user granted access to each of the department's resources. This information must be retained along with the access request.

1.1006.97 Managing System Access for Critical Systems (Reviewing and Managing System Access)

A. Reviews of system accounts must be performed, at a minimum, on semiannual basis for user accounts with privileged/administrator access as well as for accounts with access to data classified as Elevated or High. Regular user accounts and accounts with access to modify or delete data classified as Low or Moderate must be reviewed at least annually.

B. User access must be reviewed by department managers or system owners who are familiar with system users' job duties and the access required to perform those job duties.

C. Users that no longer require their assigned access rights must be identified and have those access rights disabled or deactivated.

D. Disable or delete any accounts that are inactive or assigned to individuals that are no longer working for the department. For critical systems, employees' access rights will be modified, as appropriate, by the close of business on the same day.

E. Verify that privileges are assigned to individuals based on job classification and function, also known as role-based access control (RBAC).

F. User System Access Audits will be documented and maintained by UMDPS IT Personnel.