Information Systems Security and Use

Section: 1.1006
Effective Date: June 10, 2011
Amended: September 24, 2015

1.1006 Information systems security and acceptable use

A. This directive defines the Information System Security responsibilities and acceptable use rights for employees, guests, vendors and contractors of the University of Baltimore's information system resources. Information systems include all platforms and 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 granted access to the UB network and information systems, including but not limited to full and part-time employees, temporary workers, contractors, and those employed by others to perform University work, are covered by this policy and will comply with this and associated policies, procedures and guidelines.

C. All users are expected to conduct themselves in a legal professional, fair, considerate, and ethical manner using the University of Baltimore's information system resources. Employees should use all information system resources (i.e., computers, radios, mobile data computers, and telephones) responsibly and only for its intended function. Users should keep all equipment clean and in good operating condition. More specifically, the computers made available to UBPD personnel to perform assigned duties MUST never be used for any purpose other than security and/or law enforcement inquiries. Example, the METERS computer and/or Toughbook/pad interacts with the Maryland State Police, CJIS, NCIC, and the Baltimore Police Department. As responsible custodians of this information, visiting inappropriate, non-security/law enforcement related websites is prohibited – this practice provides viruses a gateway to critical UBPD infrastructure; severe disciplinary action will be taken against violators of this policy. This policy applies to ALL UBPD desktop, laptop computers, and mobile data computers. The use of portable storage devices (flash drives) on ANY UBPD computer must receive verbal approval from the immediate supervisor or OIC. If a supervisor/OIC is not immediately available DO NOT insert flash drive until authorization is obtained. Operation of these devices must be limited to law enforcement practice and use.

D. To be clear, inappropriate use of these devices or failure to obtain approval will result in serious disciplinary action that may include termination.

1.1006.02 User Access Responsibilities

A. Employees will comply with The University of Baltimore'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 guidelines may be brought to the attention of the Office of Technology Services (OTS), the university's council, or the University of Baltimore's Hoffberger Center for Professional Ethics.
   1. All agency computers and computer systems are the property of the University of Baltimore.
   2. All computer systems and information stored within the computer systems are also the property of the University of Baltimore 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 agency. The use of these resources must be conducted according to the policies, standards, and procedures instituted by the agency or on its behalf. The unauthorized use or disclosure of information provided by these data processing systems may constitute a violation of agency, State, and/or Federal laws which will result in disciplinary action consistent with agency policies and procedures.
   1. University of Baltimore 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 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 and must notify the OTS should it be determined access rights need to be modified.

C. General Use Guidelines
   1. Users are to log off the network at the end of each day and logout of secure applications when away from their desk, office or common computer being used.
   2. Users should store important files on their network drive (M) where files are backed up daily. Items saved on the C drive of computers **are not backed up**.
   3. All individual user passwords must be kept confidential. Users are never to share passwords with other users.
   4. Users are to change their passwords when required or as necessary.
   5. No employee is to use a computer logged on by another or use a computer they do not have permission to use.

1.1006.04 Rights of Information Ownership

A. The university and the agency retains the rights of ownership to all information systems resources including hardware, software, functionality, data, and related documentation developed by the

university or agency users on behalf of the university or agency and all university and agency information contained therein.

B. Systems resources remain the exclusive property of the University of Baltimore and/or the agency, unless otherwise prescribed by other contractual agreements.

1.1006.06 Internal Network and Internet

A. The Internet is a world-wide collection of interconnected computer networks. The agencies local network **UB Police** is the University's 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, 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 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 agency.
   5. **When sending or forwarding e-mail via agency e-mail accounts, Users shall identify themselves clearly and accurately.**
   6. **Anonymous or pseudonymous posting is expressly forbidden, unless otherwise allowed by law to make anonymous postings**.
   7. **Users are responsible for protecting the university and the agency's sensitive information by following the university's policies and procedures.**

D. Users have a responsibility to ensure, to the best of their ability, that all public information disseminated and the Information 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 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 University policies (such as private/personal fund raising, profit-making, political activities, etc.) is prohibited**, **without written authorization from the University.**

G. **Mass emailing by employees that do not have authorization to agency business is prohibited.**

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

I. **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.**

J. **Users shall not access or attempt to gain access to any computer account 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.

K. **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 UBPD business.** The use of UBPD provided computer or **any other** technology based equipment for personal entertainment purposes is prohibited.

1.1006.08 Workstation Security

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

B. The following requirements apply to office, home, or other remote access locations if utilized for UBPD 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 after working hours.
2. All Departmental (PCC, Officer's Room, Sergeant's Room) computers and computer terminals **must not be left logged on when unattended** or not in use; Example, PCO leaves PCC for a personal relief – the PCO will log off and the relieving PCO or S/O will log on. This is necessary to maintain the integrity of the UBPD computer system, and to protect the officer from unnecessary scrutiny if the computer is somehow compromised during their absence. Failure to follow this protocol will result in disciplinary action.
3. Classified or sensitive information **will 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 drive (M) where files are backed up daily, not on the C drive;
5. All individual user passwords must be kept confidential. Users should not share their passwords with other users. Users are to 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.

1.1006.10 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. Agency management shall maintain an inventory of all authorizations and use of removable storage devices. Any use must meet Removable Media Security Policy.
C. Users shall request the use of agency owned storage devices. Supervisors 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 UBPD security standards. Any incidents of misuse, theft, or loss of data must be reported to a supervisor **IMMEDIATELY.**
E. UBPD sensitive or confidential information shall not be stored at home without appropriate authorization from the user's supervisor, in consultation with the Captain. Users shall follow appropriate physical safeguards for offsite use.
F. The University of Baltimore Office of Technology Services (OTS) will control physical and digital access and securely store information system media within a controlled area.
G. All storage attached, associated with, or extracted from UBPD systems will be kept securely in an OTS designated area.

1.1006.12 Media Sanitization

A. OTS 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 are erased using the Data Eliminator HD-2 machine that uses the degaussing system prior to reissue or disposal. All disks that are being erased will be stored securely and documented.

1.1006.14 Media Disposal

A. OTS personnel will destroy storage media no longer needed or in a failed state once sanitized and approved by designated OTS management.
B. When UBPD storage is no longer needed or in a failed state the disk will be kept securely on site unit it is destroyed. Destruction will be coordinated by OTS and will be documented using OTS policy and procedures.

1.1006.16 Media Transport

A. Agency personnel protect and control criminal justice data and restrict activities with transport of such media to authorized personnel. These personnel include, but are not limited to:
    1. Sworn UBPD personnel

2. Non-sworn UBPD personnel
3. Information Technology (OTS) personnel

B. In the event the media must be transported outside of UBPD controlled facilities, UBPD will escort approved OTS personnel to a secured OTS area. Approved personnel will have successfully passed a criminal background investigation and have been fingerprinted by the State.

1.1006.18 Event Logging

A. User access to the network is logged by Active Directory (AD) or Active Directory Application Mode (ADAM) (depending on directory being used). Local machine access uses the default Windows settings for logging, which at UB includes system access.

B. At the domain level, logging of permissions changes is not turned on due to impact on performance. Access is limited to OTS personnel (Server Administration and PC Support Services (PCS) teams) and changes to permissions are made in AD via security groups. OTS privileged users are also required to sign non-disclosure/confidentiality agreements. At the local level we're using default Windows settings for logging. Compensating controls therefore are:
    1. Limited access
    2. The signing of non-disclosure agreements

C. Password changes are logged by AD or ADAM (depending on the directory being used). Locally, we're using default Windows settings for logging.

D. Privileged accounts are logged in the same way as regular accounts. Note that privileged accounts are protected with additional controls, such as removal from the password management tool, which prevents passwords for these accounts from being changed online using the password management tool or by the call center staff. Additionally, OTS privileged users are required to sign non-disclosure/confidentiality agreements.

E. Direct access to server audit logs is limited to the OTS server team. Logging of changes to audit logs, however, is not turned on (per server team) for performance reasons. Locally, we're using default Windows settings for logging and access to log files is limited to users with local admin accounts. Compensating controls for direct access to server audit logs are:
    1. Limited access
    2. The signing of non-disclosure agreements

1.1006.20 User Privacy

A. All users of the agency's information systems are advised that their use of these systems are subject to monitoring and filtering.
    1. The university reserves the right to monitor randomly and/or systematically the use of Internet and UBPD 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.) can be monitored, logged, recorded, filtered, archived, or used for any other purposes, pursuant to applicable agency policies and State and Federal laws or rules.
    3. The university reserves the right to perform these actions with or without specific notice to the user.

1.1006.22 Software and Hardware

A. All software licenses purchased by the University of Baltimore Police Department belong to the agency. As such:
   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 one wants to install any software, permission must be obtained from Office of the Chief.

B. Installation of Software or Hardware
   1. UBPD information system hardware and software installations and alterations are handled by authorized OTS personnel only. Users shall not install new or make changes to existing information system hardware or software without prior authorization through the Office of the Chief of Police/OTS.
   2. Users shall not download software from the Internet unless specifically approved through the Office of the Chief. 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 Office of the Chief and the employee's supervisor prior to purchase.
   2. Employees purchasing and having unauthorized programs, without the prior written consent of the Chief, will be subject to disciplinary action.

1.1006.24 Computer Viruses: Malware

A. It is the responsibility of each user to prevent the introduction and spread of computer viruses or other malware. All personal computers in the agency must have the provided virus detection software running at all times.
   1. Users MUST immediately contact their supervisor and contact OTS when a virus is suspected or detected; OTS will confirm the attack and ensure its removal.
   2. Users must report all information security violations to the appropriate agency supervisor, who will notify OTS and the Office of the Chief.

1.1006.26 Remote Access

A. A small number of UBPD users may be permitted to remotely connect to the university's systems, networks and data repositories to conduct Agency-related business only.
   1. Users will only be granted remote access through secure, authenticated and managed access methods and in accordance with OTS and UBPD 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 in this directive.

1.1006.28 Responsibilities of OTS

A. Responsibilities of the Office of Technology Services (OTS):

1. Maintaining a liaison with the agency to ensure off site server back-ups are conducted and maintained;
2. Keeping the UBPD computer systems running and configured properly;
3. Coordinating purchasing, installing, training, operation, maintenance, storage, moving, and reconfiguration of UBPD 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. Providing annual audits of agency computer system security issues which includes password and other access violations.

B. OTS is also responsible for creating access accounts for authorized users only.