Policy 1305

Subject

USE OF DEPARTMENTAL PERSONAL COMPUTER SYSTEMS

Date Published

10 December 2017

Page

1 of 5

By Order of the Police Commissioner

POLICY

1. **Accountability**. All Personal Computer (PC) systems owned by the Baltimore Police Department (BPD) are under the administrative control of the Information Technology Section (ITS). This includes all computers and computer equipment purchased directly by, and/or donated to, the BPD regardless of the funding source.

2. **Assignment, Placement, and Distribution**. ITS shall have control of the administrative assignment, placement, and distribution of all PCs on the BPDnet and all other BPD owned computer hardware and software. PC hardware shall not be moved or modified in any way without prior approval from ITS.

3. **Copyright Violations**. Violations of software copyright law form the basis for departmental, civil, and/or criminal sanctions.

4. **Internal Regulations**. The procedures and regulations set forth by this policy are intended for internal administrative purposes only and are not intended to create any higher legal standard of care or liability in an evidentiary sense than is created by law.

DEFINITIONS

Application Password — A password that is assigned within an application and/or document on a PC that prohibits other users from opening the application or document. Application passwords must first be registered in writing with the appropriate Commanding Officer and with ITS.

BPDnet — The BPD computer network, including PCs connected to any of the department’s Local Area Networks (LAN) or Wide Area Network (WAN).

Distribution Disk — The original program disks or CD-ROMs included with a software package at the time of purchase.

LAN (Local Area Network) — A system connecting many computers within a given area to allow them to communicate internally and externally, to share information and files, and to gain access to central network services.

Login Password — A unique password that is utilized by a user to login and gain access to a computer system. In most cases, the Login Password may by chosen by the member, and not assigned by ITS.

Login Name — The user's sequence number, or in some cases a "user name" derived from the user's last name, followed by the first letter of the user's first name.

Operating System — The software responsible for controlling the allocation and usage of hardware resources such as memory, central processing unit (CPU) time, disk space, and peripheral devices (e.g., Microsoft Windows, Windows NT, and IOS).

PC — A personal computer system.

Power-On Password — A password assigned to the hardware of a PC that prevents other BPDnet users from starting the system. Power-On Passwords must have prior approval from MIS.

WAN (Wide Area Network) — A system connecting any number of LANs.

Work Product — Any BPD document, spreadsheet, program or other electronic file that is created, produced, edited, or modified on a BPD or privately owned PC during departmental work time or off-duty.

REQUIRED ACTION

Member

1. All Work Products created by a member are considered to be for, on behalf of, and owned by the BPD.

2. Information that violates any policy, rule, regulation, or law shall not be placed on a BPD PC.

3. Any materials placed on a BPD PC that are considered obscene or profane are prohibited, unless the material(s) are pursuant to an actual law enforcement purpose, and then only with the prior notification and acknowledgement of the appropriate Division Chief and the Director, ITS.

4. Members shall not put Application Passwords or Power-On Passwords on a BPD PC without ITS approval. All application and screen saver passwords must first be registered in writing with the appropriate Commanding Officer and with ITS.

5. Members shall neither share nor give their personal Login Password to another member or any other person. Any member who believes their Login Password has become known to another person shall change the password immediately.

NOTE: All passwords shall meet regulatory requirements (as an example, your cell phone MDM requires a minimum of 4 characters with one being alphanumeric, which are different than e-mail, Novell, NCIC).

6. E-mail messages, either internal or external, are not considered confidential and may be examined upon authorization by the Police Commissioner, or designee.

NOTE: Users must keep in mind that they have no reasonable expectation of privacy with regard to any e-mail message, whether or not it is marked "Private" or "Confidential."

7. Members shall not install, modify or replace the Operating System on any BPD owned PC without prior written approval from ITS.

8. If personally owned computer software must be installed onto any BPD PC, a written request shall first be submitted to ITS via the Commanding Officer of the unit where the software is to be installed. Approval from ITS is required before installation. Proof of ownership of the software must be demonstrated, and original documentation and media must remain in proximity to the BPD PC on which it is installed.

9. To procure installation of software on a BPD PC, submit a request to ITS via official channels. The request shall include:

    9.1. The name and type of software requested and the reason for the proposed installation;

    9.2. How the software will benefit the unit;

    9.3. Which PC the software will be loaded on (include the serial number and BPD property numbers); and

    9.4. Where the Distribution Disk(s) and user's manual will be stored.

NOTE: Acceptance of the terms of the Software Licensing Agreement is required before using any software product.

10. Software shall not be copied from a BPD PC, the BPDnet, or a BPD owned Distribution Disk for use on a member's personally owned computer, or any other computer, if the duplication violates copyright or licensing laws. Software piracy is a violation of federal law.

11. If BPD owned computer hardware or software must be installed in or on any personally owned PC, an Administrative Report requesting such installation must first be submitted to and approved by ITS.

12. Store all important files and documents on the server, either in the "private" directory (which is identified by the user's sequence number) or in a directory "shared" with other related users. Data stored in a user's "private" directory on the server is not accessible to other BPDnet users. Data stored in a user's "shared" directory on the server is accessible to other users within the same network group. Documents and/or files stored in the home directories will be secure from other BPDnet users.

    12.1. Users must keep in mind that they have no reasonable expectation of privacy with regard to any item stored in their "private" directory.

    12.2. Documents and/or files that are not stored on the server will not be backed up or secured by ITS. The user is solely responsible for backing up data not stored on the server.

13. When a PC or BPDnet malfunction or problem occurs, notify ITS at 410-396-2074. Business hours are Monday through Friday, 0800 ─ 1630 hours, and Tuesday through Saturday,1900 – 0300 hours.

Commanding Officer

Approve/Disapprove requests for specific software and/or hardware installation for members assigned to your command, and forward approvals to ITS. ITS will be the final arbiter concerning whether the software/hardware is appropriate and/or compatible for installation.

Information Technology Section

1. Analyze the overall needs of the BPD to determine changing computer hardware and software requirements and prioritize the needs by order of urgency or importance.

2. Determine the assignment, placement, distribution, and redistribution of PCs.

3. Provide computer hardware and software solutions consistent with available funds.

4. Ensure that grant-funded computer equipment is utilized and distributed strictly and exclusively within the grant guidelines. Upon expiration of a grant-funded program, redistribute computer equipment purchased under the grant, if appropriate and no longer necessary for the continuance of the program.

5. Assign a network user Login Name and initial Login Password to all appropriate BPD personnel, based on command input. BPDnet users will be required to change their password upon their first login and periodically thereafter.

6. Back-up all directories on the server daily.

7. Periodically monitor and audit the entire system. If any unauthorized software, hardware, or any Power-On and/or Application Passwords are discovered, ITS personnel will remove the software, hardware, and/or password from the PC and report the discovery to the ITS Director.

8. Annually inspect and validate all system accounts. Document all user account inspections and validations by means of administrative reporting to be kept on file for auditing purposes. The written reporting shall include certification that all active user accounts are valid and authorized.

9. Maintain a Security Incident Response Plan and current Computer Security Incident Response Team (CSIRT) call-up roster. Implement the Cyber Security Incident Response protocol and assume administrative guidance over the response to any security incident. Ensure that all on-duty ITS members are properly trained on CSIRT protocols and escalations.

ASSOCIATED POLICY

Policy 1306, *BPDnet and Internet Usage Policy*

RESCISSION

Remove and destroy/recycle Policy 1305, *Use of Departmental Personal Computer Systems*, dated, 15 March 2017.

COMMUNICATION OF POLICY

This policy is effective on the date listed herein. Each employee is responsible for complying with the contents of this policy.