

---

## COMPUTER PASSWORD POLICY

---

**1. PURPOSE AND SCOPE.** This Circular provides guidelines, responsibilities and procedures for creation and administration of computer passwords at the Bureau of Engraving and Printing. These guidelines are the minimum security requirements for passwords and apply to all persons using any Bureau computing device, including workstations, laptop computers, servers, mainframe computer, personal electronic devices (PED), and networks.

**2. POLICY.** It is the policy of the Bureau of Engraving and Printing to authenticate users who access Bureau networks, computers, and Bureau information residing on these or other Bureau authorized information systems, and to secure these resources from unauthorized access. The Bureau will comply with Federal regulations and standards and with Department of the Treasury policies in providing access controls which are appropriate for the level of the information protected. BEP will also maintain management controls and physical safeguards which are appropriate for the level of information protected.

### 3. REFERENCES.

a. "Password Usage," Federal Information Processing Standard (FIPS) Publication No. 112, NIST, May 1985.

b. "Automated Information Systems and Network Security," Department of the Treasury Security Manual, TD P 71-10, Section IV.

c. "BEP Internet Policy," BEP Circular No. 70-04.7, June 6, 2001.

d. "BEP Email Policy," BEP Circular No. 70-04.6, May 21, 2001.

e. "BEPMIS User ID and Password Procedures," BEP Circular No. 10-08.18, September 20, 1994.

f. "Management Information System Security Profiles," BEP Circular No. 10-08.14, May 22, 1997.

### 4. SUPERSESSION.

"Computer Password Policy," BEP Circular No. 10-08.11, **June 11, 2001**, and "**Computer Access Control Policy**" BEP Circular 10-08.18, **June 11, 2001** are superseded.

**5. DEFINITIONS.**

a. Password – a sequence of characters used in conjunction with some type of user identification to authenticate the identity of the computer user and also to control access to systems and information.

b. User – any person who is allowed the right of access to computer systems or networks. The level of access and the systems, capabilities or data that the user can access will depend on the individual's job requirements and, in some cases, position sensitivity.

c. Administrator – an individual who has additional system rights, such as the ability to set configurations, make modifications and also perform functions such as allowing access. The Bureau recognizes two categories of administrators. The first category is system administrators, who administer major systems such as the Internet and intranet, the mainframe computer, and the desktop operating environment. In addition, there are a number of local administrators who manage and monitor systems which support specialized functions of an office or similar operating area and have a well-defined and limited number of users.

**6. RESPONSIBILITIES.**

a. The user shall:

(1) create a new password immediately upon receipt of an initial or reset password. This password should contain a combination of characters that make it difficult to guess, and it should meet the requirements for a valid password shown in Appendix A. Common names, words related to the Bureau, birth dates or other words or phrases related to the user's personal identity should not be used. This password will be used when logging onto the system for which the user has access.

(2) protect his/her password from others. The user is not authorized to share his/her password with anyone else regardless of their position. The user should memorize the password and not post or store it where others may find it. Passwords, encrypted or unencrypted, should not be stored on any computer media.

(3) not use anyone else's password.

(4) manually enter the user identification and password when logging onto the system.

(5) not enter a password into any file, program, record, or script for the purpose of creating an automated log-in feature. This means that the creation of "macro-" or other files or programs that automatically enter system identification and passwords is prohibited. These programs bypass the requirement to key in the user identification and password each time when logging on, and are never secure.

**CIRCULAR**

No. 10-08.11

REVISED

DATE May 31, 2002

(6) change the password when required, immediately after receipt of an initial or reset password, at least every 90 days. The password should also be changed when requested by the system administrator or Information Technology Security Division (ITSD) representative or, at the Western Currency Facility (WCF), a Management Control Branch (MCB) representative (for BEPMIS including VACS) or an ADP and Telecommunications Branch (ADP) representative (for other than BEPMIS). Immediately change their password and notify the Help Desk, the system administrator, the ITSD, or the Management Control Branch or ADP and Telecommunications Branch in Fort Worth if they suspect the password has been compromised.

(7) not reuse the same password for a period of at least 6 months after it has been changed.

(8) provide identification when requesting that his/her password be reset. Approved forms of identification include a valid personal identification number (PIN) or in-person presentation of a Bureau badge.

(9) notify the system administrator, the Help Desk, or the ITSD in Washington; or notify the MCB for BEPMIS (including VACS), or the ADP and Telecommunications Branch for non-BEPMIS in Fort Worth of any unusual occurrences during logging in, signing off or during use of the computer.

b. Supervisors shall:

(1) ensure that employees know how to create, use and protect a password and how to protect Bureau information from unauthorized access.

(2) periodically review computer use policies with employees to ensure that access and other rules and regulations are being followed.

(3) ensure that instances of suspected password compromise are reported to ITSD.

c. The Support Services Division (Washington, D.C. facility) and the ADP and Telecommunications Branch (WCF) shall:

(1) issue initial passwords for all Internet access and BEP computer and network accounts, except mainframe accounts according to the Requirements for Valid Passwords (see Appendix A).

(2) authenticate the user and protect passwords from disclosure by validating the user's personal identification number (PIN) or in-person identification using a valid BEP badge. Passwords shall be provided only and directly to the account owner.

(3) report instances of suspected password compromise to ITSD.

d. The Chief, Office of IT Operations shall:

(1) ensure that a system administrator is designated for each system that resides on any Bureau computing device or is part of the Bureau-wide IT architecture.

(2) report instances of suspected password compromise to ITSD.

e. System Administrators in Washington and Fort Worth shall:

1) change all default or vendor passwords, including those for software packages and maintenance accounts, as soon as possible after acceptance of the software.

(2) report instances of suspected password compromise to ITSD.

f. The Customer Support Division (Help Desk) in Washington and the Management Control Branch (for BEPMIS including VACS) and ADP and Telecommunications Branch (for other than BEPMIS) shall:

(1) accept and process requests to reset passwords for mainframe (BEPMIS) and network accounts according to the Password Reset Responsibilities Matrix (see Appendix A). Handle password resets for suspended accounts and for unsuspended accounts (forgotten passwords). Accounts are suspended after 30 days of inactivity or after 3 failed logon attempts.

(2) authenticate the requestor as the account's authorized user prior to processing the password reset. This may be done by validating the user's personal identification number (PIN) or, if in-person, by presenting a valid BEP badge.

(3) maintain account security by providing passwords directly to the account owner only.

(4) report instances of suspected password compromise to ITSD.

g. The Information Technology Security Division shall:

(1) issue initial mainframe passwords.

(2) reset all passwords for mainframe accounts that have been administratively suspended (asuspend). This suspension occurs when an account is temporarily suspended or inactive for over 180 days.

(3) maintain account security by providing passwords directly to the account owner only. Authenticate the requestor as the account's authorized user prior to providing the password. This may be done by validating the user's personal identification number (PIN) or through in-person identification using a valid BEP badge. Passwords shall be provided only to and directly to the account owner.

(4) serve as a backup resource for resetting passwords for mainframe accounts.

(5) monitor the use of passwords for all authorized users, including system administrators, for compliance with Bureau policy.

# CIRCULAR

No. 10-08.11

REVISED

DATE May 31, 2002

---

(6) deny access to BEP systems when necessary, such as in cases of repeated and intentional misuse of passwords.

(7) periodically test password strength and use, review access, and coordinate training of users and administrators on password use and policy.

(8) ensure activity related to system security (e.g. failed logon attempts, password resets) is recorded in system logs.

(9) monitor system logs.

**7. OFFICE OF PRIMARY RESPONSIBILITY.** Associate Director (Chief Information Officer).

**<SIGNED>**

Ronald W. Falter  
Associate Director (CIO)

Distribution E

## Appendix A

Requirements for Valid Passwords	
Account Type	Valid Password Length
PC/Network	At least <b>8</b> Alphanumeric and/or special characters
Internet	At least <b>8</b> Alphanumeric and/or special characters
PC/Network Admin	At least <b>12</b> Alphanumeric and/or special characters
Mainframe	<b>8</b> Alphanumeric characters, no back to back repeating characters
Portable Digital Assistants (PDAs)	Varies depending on device, ITSD will set standards for approved devices

Password Reset Responsibility Matrix					
	Mainframe (BEPMIS)		PC/Network		PDA
	Day Shift	Other Shifts	Day Shift	Other Shifts	All Shifts
Washington, D.C.	Help Desk 874-3010	Help Desk	Help Desk	Help Desk	Depends on Device
WCF	Management Control Branch	Help Desk	ADP and Telecommunications Branch	Help Desk	Depends on Device