
COMPUTER ACCESS CONTROL POLICY

1. PURPOSE AND SCOPE. This policy sets the minimum security requirements for access to the Bureau of Engraving and Printing's computer systems, other computing devices, and networks, and the data that resides on these or other systems. It applies to all computing resources, networked and standalone, and to all persons who use them. Additional information on specific procedures is available in the documents listed in the References paragraph.

2. POLICY. It is the policy of the Bureau of Engraving and Printing to protect the information stored, processed, and transmitted by computer systems and networks by providing access controls which are appropriate for the level of the information protected. Access controls shall provide timely and reliable access to Bureau networks and computers for authorized users while securing these resources from unauthorized users. The Bureau will comply with Federal regulations and standards and Department of the Treasury policies in providing appropriate access controls, management controls and physical safeguards.

3. REFERENCES.

- a. "Automated Information Systems and Network Security," Department of the Treasury Security Manual, TD P 71-10, Chapter VI, Section IV.
- b. "BEP Internet Policy," BEP Circular No. 70-04.7, June 6, 2001.
- c. "BEP Email Policy," BEP Circular No. 70-04.6, May 21, 2001.
- d. "Management Information System Security Profiles," BEP Circular No. 10-08.14, May 22, 1997.

4. SUPERSESSION.

"Computer Access Control Policy," BEP Circular No. 10-08.18, **June 11, 2001** is superseded.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.

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

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 depends on that individual's job requirements and, in some cases, position sensitivity.

c. Administrator – administrators are individuals who have additional system rights and have 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 are responsible for major systems such as the Internet and intranet, the mainframe computer, and the desktop operating environment. The second category includes a number of local administrators who manage and monitor systems which support specialized functions of an office or a similar operating area and which have a well-defined and limited number of users.

7. RESPONSIBILITIES.**a. Users shall**

(1) complete the appropriate access request form and acceptable use agreement and obtain approvals as shown in the Appendix A.

(2) notify the appropriate authorities if job description or duties change, as this may affect access privileges or access requirements. At the Washington, D.C. facility, notify the IT Security Division (ITSD). At the Western Currency Facility (WCF), notify the Management Control Branch (MCB) for mainframe (e.g. BEPMIS, VACS) or the ADP and Telecommunications Branch (ADP) for non-BEPMIS.

(3) protect their accounts and the information and systems to which they have access from unauthorized access. Users are not authorized to share their access privileges with anyone else regardless of their position.

(4) be accountable for all activity that occurs using their accounts. Access only those systems, files, networks, or programs necessary to perform management-approved responsibilities. Access does not equate to authority. Do not use another person's account or associated access privileges.

(5) notify the appropriate authorities of any unusual account activity or occurrences during log-on or sign-off or during use of your computer. At the Washington, D.C. facility, notify the system administrator, the Help Desk, or the ITSD. At the Western Currency Facility, notify MCB (for mainframe, e.g. BEPMIS, VACS), or the ADP and Telecommunications Branch (for non-mainframe).

(6) identify sensitive and/or Privacy Act data and contact ITSD to ensure proper access control measures are implemented

(7) log off, if leaving a computer terminal unattended or, if the computer is not shared with others, log off or use the lock workstation feature or a password protected screen saver.

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

(8) not access or permit access to any Bureau computing resource from a remote location unless explicitly authorized in writing and approved at the Associate Director level and by ITSD.

(9) promptly report all violations of this policy to the ITSD, or for the Western Currency Facility, to the MCB.

b. Network Domain Administrators shall

(1) use their domain administrator account for administration duties only. Do not use the administrator account for standard user privileges (e.g. e-mail or the Bureau network).

(2) produce and retain logs for monitoring and auditing system access activity.

(3) require a written request authorized by the system/data owner's Office Chief or higher, and the Manager, ITSD, prior to providing access to information protected by access controls.

c. Supervisors shall

(1) protect Bureau systems and information by approving the appropriate level of network, application system and file access for users based on job requirements and need to know. Ensure that employees' access authorizations maintain appropriate separation of duties. Ensure that the appropriate access request and acceptable use agreements have been submitted by the employee and that the information and access levels indicated are correct. (See BEP Circular 10-08.14, "Management Information System Security Profiles," for instructions on creating or changing Office profiles.)

(2) ensure that users have the proper level of personnel security clearance for the information they will be accessing.

(3) perform reviews of and re-certify users account access permissions at least annually.

(4) promptly notify the ITSD or the Systems Support Division (for Washington, D.C. facility), or the MCB and ADP and Telecommunications Branch, when an employee transfers to a different job or organizational unit (e.g. Division or Office), if access requirements change, or if an employee is suspended or leaves Bureau service.

(5) ensure that appropriate access controls are implemented for all Bureau information stored, processed, or transmitted in electronic form.

d. The Systems Support Division (Washington, D. C. facility) and the ADP Telecommunications (WCF) shall:

(1) process approved requests to issue accounts for all BEP computers (other than the mainframe) and network access, including for system administrators.

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

(2) process approved requests to update, disable or delete account access privileges.

(3) ensure that, when software is installed the default passwords are changed.

(4) process requests to create shared network directories (local shares are not supported).

e. The Management Control Branch (WCF) shall:

(1) approve requests to establish or update mainframe access for users at the Western Currency Facility based on job requirements, need to know, and maintenance of appropriate separation of duties. Ensure that the appropriate access request and acceptable use agreements have been submitted by the employee and that the information and access levels indicated are correct.

(2) periodically assess access controls and provide assistance to Bureau personnel for the design and implementation of appropriate mainframe access controls for Bureau information that is stored, processed, or transmitted in electronic form.

f. The Information Technology Security Division shall

(1) issue mainframe accounts (e.g. BEPMIS and VACS).

(2) process approved requests to delete or update mainframe account access.

(3) monitor account, system, and file usage for all users, including system administrators, for compliance with Bureau policy. In cases of repeated and intentional violations of access policy or account misuse, deny access to BEP computer systems, networks and Bureau authorized systems. Deny access after three failed logon attempts or for accounts that have been inactive for 30 days.

(4) maintain Access Profiles and BEPMIS Security Matrix in compliance with Bureau policy and within the guidelines of BEP Circular 10-08.14.

(5) assess access controls and provide assistance to Bureau personnel for the design and implementation of appropriate access controls for Bureau information that is stored, processed, or transmitted in electronic form.

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

(7) monitor system logs.

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

>**SIGNED**>

Ronald W. Falter

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

Associate Director (CIO)

Distribution: E

PC/Network Access Requests			
Type of Access	Form	Acceptable Use Agreement	Required Approvals
Standard Account	PC/Network Access Request (Attachment A)	IT Rules of Acceptable Use (Attachment B)	Requestor's Division Manager or higher, Requestors Office Chief
Special Account	Special Access Request (Attachment C)	IT Rules of Acceptable Use (Attachment B)	Division Manager, Office Chief, Manager, ITSD Manager, SSD
Internet	Internet Access Form (See Internet Policy)	Included on Internet Access Form	Office Chief or higher, CIO

Mainframe Access Requests (BEPMIS and other Mainframe Application Systems)			
Type of Access	Form	Acceptable Use Agreement	Required Approvals
Establish, Change, or Delete User's Mainframe Account Access	Request for Personnel Access Profile Change (Attachment D)	IT Rules of Acceptable Use (Attachment B)	Division Manager or higher
Dispatch (to view reports on-line)	Request for DISPATCH Access (Attachment E)	N/A	Division Manager or higher
TSO/Batch or Access to	Request for TSO/Batch Access (Attachment F)	N/A	Division Manager or higher
Establish or Change an Access Profile	Request for a Profile Structural Change (Attachment G)	N/A	System/Data Owners

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

Attachment A

Bureau of Engraving and Printing

PC/Network Access Request

Name: _____
(Print – Last, First, Middle Initial)

Date: _____

Badge Number: _____

Room Number: _____

Phone: _____

Office/Division (i.e., OITO/SSD): _____

Request for (check all that apply):

Network Account*

E-mail Account

Other (specify) _____

Justification:

I have read and agree to comply with the IT Rules of Acceptable Use.

(Requestor's Signature)

Approvals:

Manager: _____
(Requestor's Division Manager**)

Date: _____

Manager, IT Security: _____

Date: _____

Manager, Systems Support: _____

Date: _____

Request Received Date: _____

Account ID Assigned: _____

Date: _____

*Network access establishes the BEP standard user account with access to In\$ite, and the user's home folder, office folder, and directorate folder.

**This person is responsible for notifying OITO if access is to be changed or terminated for any reason (e.g., reassignment, resignation, separation, etc.).

Bureau of Engraving and Printing

Information Technology Rules of Acceptable Use

1. All Users are responsible for maintaining the security of the Bureau's information systems. All uses of BEP computing resources must comply with Federal government, Treasury, and BEP policies, and procedures. Any violation of these policies and procedures may result in administrative action, civil or criminal prosecution, or termination of employment.
2. 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 below. Do not use common names, words related to the Bureau, birth dates or other words or phrases related to the user's personal identity. This password will be used when logging onto the system for which the user has access.

Requirements for Valid Passwords

<u>Account Type</u>	Valid Password Length
PC/Network	At least 8 Alphanumeric and/or special characters
Internet	At least 8 Alphanumeric and/or special characters
PC/Network Admin	At least 12 Alphanumeric and/or special characters
Mainframe	8 Alphanumeric characters, no back to back repeating characters
Personal Digital Assistant (PDA)	Varies depending on device, Information Technology Security Division (ITSD) will set standards for approved devices

3. Protect your password(s) from being disclosed. Users are responsible for any computer activity associated with their accounts. Do not write down password(s) where others might easily find it.
4. Do not attempt to guess or discover passwords by trial and error. Such activity can be interpreted as an attempt to obtain unauthorized access.
5. If you suspect your password is known by someone else, change your password and report the suspected compromise to the appropriate authorities. At the Washington, D.C. facility, notify the Help Desk, systems administrator or the Information Technology Security Division. At the Western Currency Facility, notify the Management Control Branch for mainframe passwords (e.g. BEPMIS, VACS) or the ADP and Telecommunications Branch (ADP) for non-BEPMIS passwords.
6. Do not enter password(s) in a file or script for the purpose of creating an "autologin" feature. Passwords may not be stored, encrypted or unencrypted, on any computer media.
7. Change your password at least every 90 days or when required, immediately after receipt of an initial or reset password, when requested by the system administrator or an ITSD representative: or at the Western Currency Facility (WCF), a Management Control Branch (MCB) representative, or ADP and Telecommunications Branch (ADP) representative.
8. Do not reuse the same password for a period of at least 6 months after it has been changed.

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

9. Do not log on and let anyone else use your account or associated account privileges.
10. Do not use anyone else's account or access privileges.
11. Provide identification when requesting that your password be reset. Approved forms of identification include a valid personal identification number (PIN) or in-person presentation of a Bureau badge.
12. Notify the system administrator, the Help Desk, or the ITSD of any unusual occurrences during logging in or signing off or during use of the computer. At the WCF, notify MCB.
13. Log-off any time you leave your computer unattended. If you do not share a computer, you may lock it or use a password protected screen saver.
14. Use proper log-off procedures. Do not shut down the computer. Leave the electrical power turned on to the computer. You may turn off the monitor using the monitor on/off power button.
15. Access and use only those BEP network, personal computer (PC), or other computing resources for which you are authorized. Do not attempt to access resources for which they have not received explicit authorization.
16. Users may not download or install any software, install hardware, exchange system components, modify any system configuration files, or connect hardware to the network. Do not use unauthorized software or hardware.
17. Protect information technology resources from theft, destruction, misuse, and physical hazards such as liquids, food, smoke, staples, paper clips, etc.
18. Do not disclose telephone number(s) or procedures for system access from a remote location.
19. BEP network and IT resources may be used for official and authorized use only.
20. Users are responsible for protecting any information used and/or stored by their account. Users must report any incidents of possible misuse, suspected viruses or IT security incidents or weaknesses in IT security to the Help Desk or at the WCF to MCB or ADP.
21. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized Bureau user access to a Bureau resource; obtain extra resources beyond those allocated; circumvent Bureau computer security measures; or gain access to any system for which proper authorization has not been given.
22. Users shall refer to the BEP Internet and Electronic Mail policies for guidance on the appropriate use of those services.
23. To protect the BEP computer resources from unauthorized use and to ensure that the system is functioning properly, activities are monitored and recorded, and are subject to audit. Use of this system is expressed consent to such monitoring and auditing. Any unauthorized access or use of this system is prohibited and could be subject to disciplinary action and criminal and civil penalties.

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

- 24. Identify all sensitive information that you will be placing on the system, and any equipment used to process sensitive information to the Information Technology Security Division, so appropriate security measures can be implemented. BEP systems are sensitive but unclassified. Classified information (Top Secret, Secret, and Confidential) may not be processed, entered, or stored on any BEP system.
- 25. I understand that BEP reserves the right to terminate my access at any time.
- 26. Managers shall immediately notify the system administrator or the Information Technology Security Division when there is a change of an employee's duties or employment status or organizational unit and/or when access to the system is no longer required.

User Agreement	
I have read, understand, and agree to follow the Bureau of Engraving and Printing Information Technology Rules of Acceptable Use. I understand that any violation of these policies and procedures may result in administrative action, civil or criminal prosecution, or termination of employment.	
_____	_____
User's Signature	Date

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

Attachment C

Bureau of Engraving and Printing

Special Access Request

Name: _____
(Print – Last, First, Middle Initial)

Date: _____

Badge Number: _____

Room Number: _____

Phone: _____

Office/Division (i.e., OITO/SSD): _____

Describe special access requirement:

Justification:

I have read and agree to comply with the IT Rules of Acceptable Use.

(Signature)

Approvals:

Manager: _____
(Requestor's Division Manager*)

Date: _____

Manager, IT Security _____

Date: _____

Manager, Systems Support _____

Date: _____

Request Received Date _____

Account ID Assigned _____

Date: _____

*This person is responsible for notifying OITO if access is to be changed or terminated for any reason (e.g., reassignment, resignation, separation, etc.).

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

Attachment D

BEP FORM 8331
ORIG. 9-97

REQUEST FOR PERSONNEL ACCESS PROFILE CHANGE (G12PIDMS) (See reverse for instructions)

I. USER'S NAME

II. USER'S BADGE NO.

III. USER'S JOB TITLE

IV. USER'S OFFICE

INITIATOR

INITIATOR'S PHONE NUMBER

V. ACTIONS TO BE TAKEN

___ ADD USER TO PROFILE(S): _____

___ CHANGE USER PROFILE(S) FROM: _____ TO: _____

___ DELETE USER FROM PROFILE(S): _____

___ CHANGE USER ID TO: _____

___ CHANGE USER NAME TO: _____

___ DELETE USER FROM BEPMIS

FOR VACS, KCS AND SACS ACCESS ONLY

REQUIRES SIGNATURE OF OFFICE OF SECURITY PROJECT MANAGER

___ VACS (VISITOR ACCESS CONTROL) ___ KCS (KEY CONTROL SYSTEM) ___ SAC (SECURITY ACCESS CONTROL)

OFFICE OF SECURITY PROJECT MANAGER

(SEE REVERSE SIDE FOR ACCESS GROUP NO. FOR VACS, KCS AND SAC)

COMMENTS: _____

VI. ACCESS APPROVED BY OFFICE CHIEF/DIVISION MANAGER

SIGNATURE: _____ TITLE _____ DATE _____

As the approving official, I accept full responsibility for insuring that the actions to be taken are correct and will notify OITO immediately when user's access should be terminated, for reasons such as reassignment, resignation, separation, etc.

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

FOR IT SYSTEMS SECURITY DIVISION USE ONLY

DATE RECEIVED: _____

DATE USER NOTIFIED: _____

DATE IMPLEMENTED: _____ BY _____

DATE VERIFIED: _____ BY _____

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

Attachment D

SPECIFY GROUP NUMBER REQUIRED WHEN ADMINISTING THE FOLLOWING ACCESS:

VACS	KCS	SACS
-----	-----	-----
-----	-----	-----
-----	-----	-----
-----	-----	-----
-----	-----	-----

INSTRUCTIONS FOR COMPLETING REQUEST FOR PERSONNEL ACCESS PROFILE CHANGE FORM

- I. USER'S NAME: USER'S NAME: CLEARLY PRINT USER'S FULL NAME. IF USER'S NAME HAS CHANGED PLEASE INDICATE UNDER ACTIONS TO BE TAKEN.
- II. USER'S BADGE: PRINT THE NUMBER THAT APPEARS ON THE FRONT OF THE USERS BADGE. IF USER'S BADGE NUMBER HAS CHANGED PLEASE INDICATE UNDER ACTIONS TO BE TAKEN.
- III. USER'S JOB TITLE: PRINT THE PERSON'S JOB TITLE FOR VERIFICATION OF APPROPRIATE PROFILE ACCESS.
- IV. USER'S OFFICE: USER'S PRESENTLY ASSIGNED OFFICE
- V. PLACE BY THE DESIRED COURSE OF ACTON TO BE TAKEN.
- VI. APPROVING OFFICIAL SIGNATURE: TITLE AND DATE: MUST BE SIGNED AND DATED BY THE USER'S OFFICE CHIEF OR DIVISION MANAGER.

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

Attachment E

Bureau of Engraving and Printing

Request for Dispatch Access

Name: _____
(Print – Last, First, Middle Initial)

Date: _____

Badge Number: _____

Room Number: _____

Phone: _____

Title: _____

Office/Division (e.g. OITO/SSD): _____

Bin Number: _____

Reports Required: (Use reverse side for additional reports)

_____	_____
_____	_____
_____	_____

(Requestor's Signature)

Date: _____

Comments

Approval

Signature: _____ **Title** _____
(Office Chief /Division Manager*)

Phone: _____

*This person is responsible for notifying OITO if access is to be changed or terminated for any reason (e.g., reassignment, resignation, separation, etc.).

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

Attachment F

Bureau of Engraving and Printing

Request for TSO/Batch Access

Name: _____ Date: _____
(Print – Last, First, Middle Initial)

Badge Number: _____ Room Number: _____ Phone: _____

Title: _____

Office/Division (e.g. OITO/SSD): _____

Indicate Required Applications (i.e., TSO, Batch, etc.):

Indicate Data Set Names (DSN) and Access Level (Read, Update, Create, All)

(Requestor's Signature) Date: _____

Comments

Approval

Signature: _____ Title _____
(Office Chief/Division Manager*)

Phone: _____

*This person is responsible for notifying OITO if access is to be changed or terminated for any reason (e.g., reassignment, resignation, separation, etc.).

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002

Attachment G

Bureau of Engraving and Printing

Request for Profile Structural Change

Profile Name: _____

Profile Office: _____

Initiator's Name: _____

Phone: _____

Delete Profile

List Applications and Transactions to be added or modified

<input type="checkbox"/> Add Profile		<input type="checkbox"/> Modify Profile			
Application	Transaction	Add		Delete	
Application	Transaction	Application	Transaction	Application	Transaction
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

Comments

Approval: Requires Signatures of all Project Managers
(Initiating Office is responsible for ensuring all approval signatures are completed)

_____	_____
<i>Manager, Enterprise Systems Division (OSD)</i>	<i>Date</i>
_____	_____
<i>Project Manager, Purchasing Systems (OP)</i>	<i>Date</i>
_____	_____
<i>Project Manager, Product Accountability Systems (OMC)</i>	<i>Date</i>
_____	_____
<i>Project Manager, Security (OS)</i>	<i>Date</i>
_____	_____
<i>Project Manager, Financial Systems (OFM)</i>	<i>Date</i>
_____	_____
<i>Project Manager, Production Management (OPM)</i>	<i>Date</i>

Concurrence

_____	_____
<i>Project Manager, IT Security Division (OITO)</i>	<i>Date</i>

For IT Security Division use

Date Received: _____ Date Implemented: _____ By: _____

CIRCULAR

No. 10-08.18

REVISED

DATE May 31, 2002
