

DATE June 6, 2001

---

**BUREAU OF ENGRAVING AND PRINTING  
INTERNET POLICY**

---

**1. PURPOSE.** This Policy defines responsibilities and provides guidance for the use of the Internet. The objective is to promote economical, effective and efficient research, communication and data gathering, and ensure security of Bureau information technology and communication systems.

**2. SCOPE.** This Policy is applicable to all Bureau of Engraving and Printing (Bureau/BEP) employees, contractors and others who access the Internet through Bureau devices or while in a duty status or on Bureau premises.

**3. BACKGROUND.** The Internet is a worldwide alliance of public networks that employ a common set of protocols for communicating information. It provides tremendous benefits to Bureau users by offering increased access to a variety of information resources for official business. This access also poses significant security risks related to a number of external threats, which may result in loss of services, corruption of data, or theft of sensitive information.

**4. REFERENCES.**

Department of the Treasury Information Technology Manual, December 1998.

“Treasury Information Technology (IT) Programs,” Treasury Directive TD 81-01, April 13, 2000.

Department of the Treasury Security Manual, Chapter VI, October 1992.

“Treasury Internet Use Policy,” Assistant Secretary for Management and CFO, March 11, 1998.

“Personal Use of Government Office Equipment Including Information Technology,” Treasury Directive TD 87-04, May 17, 2001.

“Remote Access to Computer Systems,” BEP Circular No. 10-08.23, May 21, 2001.

**5. SUPERSESSION.**

“Bureau of Engraving and Printing Internet and Electronic Mail Policy,” BEP Circular No. 70-04.4, May 3, 1999, is superseded.

DATE June 6, 2001

**6. DEFINITIONS.**

a. Official Use refers to use of resources for activities which directly or indirectly support the Bureau's or the Department of the Treasury's mission and the accomplishment of related goals and objectives.

b. Authorized Use of the Internet includes official use and limited personal use. Limited personal use is permitted, providing that this is infrequent, incurs minimal expense to the Government, is during non-work time; does not involve sensitive Government information or put Government information or systems at risk; conforms with Bureau and Department of the Treasury policy; and does not interfere with official business.

c. Bureau Systems refers to computers, networks, personal electronic devices, cellular telephones with Internet capability or other devices provided by the Bureau to the user for official business, either at Bureau facilities or from a remote site.

d. Minimal additional expense refers to the use of government equipment where the employee is already provided access for official business and where the additional use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner, or paper.

e. Non-work time means when the employee is not otherwise expected to be addressing official business. This could be, for example, during lunch periods, authorized breaks, before or after duty hours.

**7. POLICY FOR OFFICIAL AND AUTHORIZED USE.** It is the policy of the Bureau to allow the use of the Internet to support the BEP mission and to accomplish its goals and objectives.

a. Internet access may be made available when:

- (1) it contributes to the accomplishment of official duties, including training which is required for job performance or compliance with law or regulation;
- (2) it is technically and financially supportable by the Office and the Bureau; and
- (3) risks to sensitive information are minimized to an acceptable level.

b. Use of the Internet is only for official use and for authorized use as defined in this policy.

c. Access to the Internet is a privilege and users shall become familiar with Bureau policy and procedures for use. Managers, Office Chiefs, and Associate Directors shall ensure that sufficient information on Bureau policies and procedures is provided to users and that training is provided if required.

DATE June 6, 2001

---

d. Use of Government equipment may be monitored and recorded. Anyone using Government equipment consents to such monitoring and shall have no expectation of privacy. If this monitoring reveals possible evidence of criminal activity or violations of policies or security procedures, evidence may be provided to appropriate Bureau management and/or law enforcement officials.

e. Any direct connection to Internet services from Bureau computers, networks, or communications services must occur through gateways and firewalls that have been approved by the Associate Director (CIO). Only Bureau issued or specifically authorized equipment may be used for Internet communications. Personally owned computers, hand-held electronic devices or cell telephones shall not be connected to or used with Bureau communication systems or Bureau devices.

f. Employees, contractors, and other users shall exercise judgment and discretion in their use of the Internet. This includes ensuring that personal use does not interfere with official business and that communications are not disruptive to the work place, do not reflect negatively on the Bureau or the Government, do not have the appearance of inappropriate use of Government resources, and do not violate the Public Trust.

g. All users must be aware of the continual threat of compromise to Bureau systems. Unprotected connections to the Internet, unauthorized communication over the Internet, or downloads of unauthorized information may compromise BEP security. If there is a suspicion of a system compromise, the user should stop using the computer immediately and contact the Help Desk.

h. Only Microsoft Outlook e-mail is authorized for Bureau users. This means that web browser e-mail, such as Hotmail, may not be used to send or receive e-mail using BEP systems.

i. There is a great deal of information available through the Internet which can benefit the Bureau and benefit Bureau users in the performance of their duties. However, Bureau users must honor legal protections of the information, such as "intellectual property [rights], copyrights, trademarks, and software licenses."

j. Remote access to Internet services from Bureau provided computers or other devices must employ appropriate security mechanisms which are consistent with the sensitivity of the information at risk, Bureau and Department of the Treasury policy. This includes, at a minimum, only access through encrypted devices such as Virtual Private Networks (VPN) or dial-up access through the Bureau firewall. Computers using VPNs will have a personal firewall installed that is approved by the Information Technology Security Division.

DATE June 6, 2001

---

k. Limited personal authorized use of the Internet shall be of reasonable duration and frequency and made during the user's personal time, such as lunch periods or official breaks. Authorized personal use of the Internet shall not:

- (1) Adversely affect the performance of official duties.
- (2) Place an excessive burden on BEP communications systems or have an adverse impact on the mission or operations of the Bureau.
- (3) Involve the creation, downloading, viewing, storage, copying or transmission of pornographic, sexually oriented, or obscene language or materials.
- (4) Violate any Bureau, Treasury, or Government law or regulation.
- (5) Involve the pursuit of private commercial business activities or profit-making activities.
- (6) Be used to conduct any activity that would adversely affect the United States Government.
- (7) Result in more than minimal expense to the Government.
- (8) Be used to support outside fund-raising activities; endorse any product or service; participate in any lobbying activity; or engage in any prohibited partisan political activity.
- (9) Be conducted in a manner that may be misrepresented as official business.
- (10) Be used to access hacker sites or to gain unauthorized access to other systems.
- (11) Be used to access sites that promote illegal activities including, but not limited to, illegal gambling, illegal weapons or terrorist activities.
- (12) Involve the creation, downloading, viewing, storage, copying or transmission of offensive materials, such as hate speech or material that demeans others on the basis of race, creed, religion, color, sex, disability, national origin or sexual orientation.
- (13) Involve the downloading, copying or playing of computer games.

DATE June 6, 2001

---

**8. RESPONSIBILITIES.**

a. Associate Directors, Plant Managers and Office Chiefs shall:

(1) ensure that access to computer equipment and authorization to use the Internet is provided to employees when necessary to accomplish the mission of their organization.

(2) ensure that training is provided users in the appropriate use and security of Bureau computer resources, and accountability and responsibility for electronic data downloads and dissemination.

(3) ensure that necessary safeguards are in place to protect the availability, integrity and confidentiality of systems for their operation units.

(4) identify and monitor appropriate management controls and technical safeguards for Internet access assignment and usage.

b. Users shall:

(1) ensure that they understand the policies and rules for use and security of the Internet.

(2) follow the access policies and the use policies to protect Bureau systems and documents and their rights to utilize the systems.

(3) read the "Internet Access Agreement" (Attachment 1) and complete the "Internet Access Form" (Attachment 2) when applying for internet access and agree to comply with the provisions of Bureau policy.

**9. SANCTIONS FOR MISUSE.** Unauthorized, improper, or insecure use of BEP Internet access may result in suspension of privileges, disciplinary action (up to and including termination), and/or criminal prosecution depending on the nature and severity of the misuse.

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

<SIGNED>

Ronald W. Falter

Associate Director (Chief Information Officer)

Distribution E

DATE June 6, 2001

## ATTACHMENT 1

**INTERNET ACCESS AGREEMENT**

Individuals granted Internet access shall be accountable for following BEP's policies and procedures on Internet use, as well as any and all laws, regulations and rules applicable to Government-owned automated data processing equipment.

The Bureau will be placing a great deal of trust in any employee granted access to the Internet. Therefore, any employee granted this access will be subject to adverse administrative and/or disciplinary action should they violate any part of this policy.

In order to obtain Internet access, the Internet Access Form (see attached) must be submitted by you through your Office Chief, Plant Manager (Washington or WCF) or Associate Director to the Chief Information Officer, Room 725-A. Both you and the individual it was submitted through should sign this form. In the "Justification" area provided on the form clearly state the reason(s) for Internet access and how this is in support of a BEP mission or need.

In addition to the above rules and regulations an individual obtaining Internet access must also agree to:

- Not divulge to nor let any other individual, under any circumstances, use your Internet user logon and password. If you believe that your user logon has been compromised, IMMEDIATELY contact the Help Desk, Office of IT Operations at (202) 874-3010. Failure to make this notification will constitute a violation of BEP's Internet Access Policy.
- Not download any file from the Internet unless it passes through BEP's standard anti-virus program. If, after downloading a file, you believe it to be corrupted with a virus, IMMEDIATELY stop using the computer and contact the Help Desk, Office of IT Operations, (202) 874-3231, who will then contact the IT Security Division. Failure to make this notification constitutes a violation of BEP's Internet Access Policy, and may result in your computer being infected with a virus along with all other computers on the network.
- Never leave your PC unattended while logged on to the Internet.
- Not divulge to nor let any other individual, under any circumstances, use your IP Address.

Physical connectivity to the Internet will be accomplished following Treasury's connection policy. This will be accomplished by BEP, using a standard desktop configuration employing Microsoft Internet Explorer and firewall (security wall), which in turn connects to the TCS carrier and from there out to the Internet. This connection strategy employs good security for BEP utilizing both a firewall and a security access program.

DATE June 6, 2001

ATTACHMENT 2



**ACCESS FORM**

**NAME:** \_\_\_\_\_ **PHONE:** \_\_\_\_\_ **ROOM:** \_\_\_\_\_  
*Please Print*

**TITLE, OFFICE, & COST CENTER:** \_\_\_\_\_  
*(Example: Manager, SSD, Office of IT Operations, 272000)*

**BEP MISSION OR NEED:** \_\_\_\_\_  
*(Examples: Counterfeit Deterrence, Ink Research, Building Security, Fixed Asset Procurement, etc.)*

**JUSTIFICATION:** *Provide a description of exactly how you will use the Internet to support the BEP Mission or Need stated above.*

---

---

---

*I certify to the best of my knowledge that the above is true and correct and that I have read and agree to adhere to the BEP Internet Policy (If not attached to this form call 4-3010 and it will be provided to you).*

**REQUESTER:** \_\_\_\_\_  
*Signature* \_\_\_\_\_ *Date*

**SUPERVISOR:** \_\_\_\_\_  
*(Office Chief or Above)* *Signature* \_\_\_\_\_ *Date*

**APPROVAL:** \_\_\_\_\_  
*Ronald W. Falter* \_\_\_\_\_ *Date*  
*Chief Information Officer*