	<h1>BPA MANUAL</h1>	Page 1110-1
	<h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Date 01/03/07


### 1110.1 PURPOSE

To provide Cyber Security policy on the use of BPA Information Technology Services. This policy applies to all personnel who have authorized access to BPA facilities and sites, including BPA federal and contractor employees and visitors. This policy applies to all BPA IT Equipment as defined in Chapter 1110.


The misuse of BPA IT Equipment and Information Technology Services poses significant risks to mission and business of the BPA.

### 1110.2 DEFINITIONS


- A. Authorized Systems Users** are BPA federal and contractor employees who have (1) undergone and passed a background security screening in accordance with current federal requirements; (2) been issued physical access; (3) been issued a logon account to the Bonneville User Domain (BUD) administrative network and/or access to any other BPA computer system or network; and (4) taken the mandatory annual Security and Emergency Management and Cyber Security training and have been validated as completing that training.
- B. Blog** is short for **web Log**. A blog is a Web page that serves as a publicly accessible personal journal for an individual, group, or community, including businesses. Typically updated daily, blogs often reflect the personality of the author.
- C. Businesslike** is practical and unemotional, purposeful and earnest; exhibiting methodical and systematic characteristics that would be useful in business.
- D. BPA Authorized Installers** are designated personnel who are authorized to install, update and remove BPA licensed software on workstation (desktop or laptop) computing devices. In addition, BPA Authorized Installers are authorized to install, modify and move BPA IT Equipment.
- E. BPA Cyber Security** is the official organization responsible for development, issuance, and enforcement of policy relating to BPA IT Equipment. Cyber Security's governance is based on federal laws, regulations, DOE Orders and BPA guidelines. All Cyber Security policies and other materials can be found on the [Cyber Security Office web site](#).
- F. BPA federal employees** are employees and supervisors employed by the federal government and BPA.
- G. BPA's Harassment-Free Workplace Policy** is provided by BPA Manual Chapter 400/700A, Appendix A.
- H. BPA IT Equipment** includes BPA's computer networks and any authorized BPA-owned computing device or component that can be attached or connected to BPA's computer network. BPA IT Equipment includes desktop computers and monitors, laptop and portable computers, software, freeware, personal digital assistants (PDAs), telephones, digital cameras, cell phones, smart phones, facsimile machines, pagers, copiers, photocopiers, printers, scanners, servers, fixed or portable storage devices (flash drives), routers, peripheral devices and multi-purpose machines (combined facsimile, printer and copier).
- I. BPA IT Support Staff** are designated personnel who are authorized to support and modify certain settings on workstation (desktop or laptop) computing devices. They are reached by contacting the Help Desk.
- J. BPA Supervisors** are BPA federal employees whose position duties include performance and/or conduct supervision of other BPA federal employees.
- K. Broadcast e-mail** is the distribution of an e-mail message to a large group (50 or more) of BPA federal and contractor employees, rather than addressing the e-mail message to a limited number of specific, individually-named BPA employees or other recipients.

	<h1>BPA MANUAL</h1>	Page 1110-2
	<h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Date 01/03/07

- L. **Chain e-mail** is the electronic equivalent of the chain letter which is a letter that explicitly directs the recipient to distribute copies of the letter to others.
- M. **Chat Room** is a web site, part of a web site, or part of an online service, that provides a venue for communities of users with a common interest to communicate in real time. Forums and discussion groups, in comparison, allow users to post messages but don't have the capacity for interactive messaging.
- N. **Configuration Settings** are persistent or saved values that describe operational parameters for software, including operating systems and hardware. Configuration settings are standardized at BPA and users are prohibited from changing those settings. For example, password changes are set for every ninety days as a standard configuration setting on the BPA administrative network.
- O. **Contractor** is defined by the Bonneville Purchasing Instructions (BPI) in part 1.8, page 1-5 as a firm or individual that currently has a contract to supply goods or services to BPA.
- P. **Contractor employee** is the employee of a contractor or is an independent contractor who has a contract with BPA to provide personnel to perform specific tasks. The contractor-BPA employee relationship is governed by the BPA contract and managed by the Contracting Officer (CO) and the Contracting Officer's Technical Representative (COTR).
- Q. **Contracting Officer (CO)** is the BPA official delegated to award binding contracts on behalf of BPA to contractors and who is responsible for appointing and Contracting Officer's Technical Representative (COTR) to administer the contract.
- R. **Contracting Officer's Technical Representative (COTR)** is appointed by the Contracting Officer by a delegation letter and administers the contract after it has been awarded. For the purposes of this Chapter, the COTR is the person who performs the day-to-day management of the contract.
- S. **Controlled Access Point** is a restricted communication boundary through which an authorized software connection can be made to a computer system on the other side.
- T. **Data** are the plural of datum and are distinct or discreet pieces of information usually formatted as data types (integer, string, etc.) and can exist electronically in database files, free text files, spreadsheet files. Data typically has no syntactical or grammatical meaning with regard to human use. Computers are capable of using such data.
- U. **Database** is a collection of information stored in a computer in a systematic way, such that a computer program can consult it to answer questions. The software used to manage and query a database is known as a database management system (DBMS).
- V. **Download** is the transfer of electronic files from a source to a destination. **Downloading** is the process of transferring electronic files from a source to a destination.
- W. **Dual Use IT Equipment** is IT Equipment that is used as both Administrative/General Purpose IT Equipment and Operational and Control IT Equipment and that may be authorized for access on the BUD administrative network with Cyber Security's authorization.
- X. **Electronic mail (e-mail)** is the exchange of computer-stored messages and attachments (files) across a network, which includes the Internet, using BPA-provided IT Equipment. The author of an e-mail message creates and sends (including forwarding of and/or replying to a received e-mail message) the e-mail message to one or more recipients by specifying the recipients' e-mail address. An e-mail author can also send a message to several recipients at once using a group e-mail address. Sent and received e-mail messages are stored in electronic mailboxes until retrieved by the e-mail user.

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 10px 0 0 40px;">Part: Information Management and Technology</p>	Page 1110-3
	Date 01/03/07	

- Y. File** is an electronic collection of binary digits (bits) and bytes (eight bits) typically characterized by a file name and an extension, although in some operating systems, a file extension is not mandatory. A file may contain text, images, motion pictures, binary data, delimited data, audio samples, Internet pages among others.
- Z. Financial Transaction** is an exchange or transfer of money from one account to another using BPA IT Equipment.
- AA. Freeware** may be commercial or non-commercial software that is available to the public at no charge. Often the licensing agreement does not contain terms acceptable to BPA. Freeware is high risk software that is typically not supported by a formal organization nor well tested or built on industry standards. It poses a significant risk to the BPA computing environment and is only permitted with Cyber Security approval. It may not be downloaded or installed without express approval.
- BB. Gambling** (gaming, betting) is to play at any game of chance for money or other stakes using BPA IT Equipment.
- CC. Guidance** is information that provides direction or advice as to a decision or course of action.
- DD. Improper Use** is that which meets the criteria of unsuitable, improper or inappropriate as defined in this Chapter and in additional Cyber Security and Employee Relations policies currently in force.
- EE. Incremental Charges** are financial charges levied on BPA that can be traced back to the specific usage incidence and the BPA federal and contractor employee responsible for incurring that charge. An example of such a charge would be calls made via cellular phone that are itemized on the monthly bill from the cell phone provider.
- FF. Information** is data that has been processed to add or create meaning for the person who receives it.
- GG. Information Technology (IT)** is any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
- HH. Internet (or Net or Web or World Wide Web)** is a global network connecting millions of computers in which users at any one computer can, if they have system permission, get information from any other computer (and sometimes communicate electronically directly to users at other computers). The interconnections between so many computers and computer users, makes the Internet a highly efficient tool for research and communication. It also poses significant vulnerability to Internet users from malicious software.
- II. IT Acquisition Review Board (ITARB)** - deleted 01-12-2007. The ITARB ceased functioning during the revision of this document.
- JJ. Non-work time** is defined as the time before an employee's workday begins, after the workday ends, or during lunch.
- KK. Operational and Control IT Equipment** is any standalone BPA IT Equipment dedicated full time for control of the BPA electrical system and is not authorized for access on the BUD administrative network without Cyber Security approval.
- LL. Password** is a confidential/secret string of characters (letters, numbers, and other symbols) used in conjunction with a user ID to authenticate an identity or to verify access authorization.
- MM. Personal Financial Transaction** is an exchange or transfer of funds (monies) on BPA Equipment to procure personal goods or services or to pay personal invoices or bills.

	<h1>BPA MANUAL</h1>	Page 1110-4
	<h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Date 01/03/07

**NN. Personal IT Equipment** is any non-BPA IT Equipment.

**OO. Personal Use** is use of BPA IT Equipment by BPA federal and/or contractor employees for non-BPA business and is defined by BPA Manual Chapter 1110A: Allowance for Limited Personal Use of BPA Information Technology Equipment.

**PP. Pornography** is pictures and/or writings of sexual activity intended solely to excite lascivious feelings, of a particularly blatant and aberrational kind such as acts involving children, animals, orgies, and all types of sexual intercourse.

**QQ. Posting** is publishing information, documents, images or audio in an online environment such as a web site, chat room, message board, blog.

**RR. Peripheral Devices** are computer devices, such as a DVD-ROM drive, flash drive or printer, that is not part of the essential computer, i.e., the memory and microprocessor. Peripheral devices can be external – such as a mouse, keyboard, printer, monitor, external hard drive or scanner – or internal, such as a DVD-ROM drive, DVD-R drive or internal modem. Internal peripheral devices are often referred to as integrated peripherals.

**SS. Personally Identifiable Information (PII)** is any information about an individual maintained by an agency, including, but not limited to education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. [Source: [Cyber Security Policy](#) BPA-20060809-001]

**TT. Presentation Settings** refer to the Microsoft Windows Screen Saver Display Properties menu which controls the appearance of the software on the display screen. Display Properties consist of settings for screen resolution and color depth, desktop background image (wallpaper), screen saver settings, configuration, and images, and appearance of windows and buttons.


**UU. The Privacy Act of 1974, 5 U.S.C. § 552a (2000)** is generally characterized as an omnibus “code of fair information practices” that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies.

**VV. Remote Access Service (RAS)** is the ability to gain authorized access to BPA IT Equipment through a controlled access point from locations outside the BPA work environment. Cisco's Virtual Private Network (VPN) is an example of software used to permit secure authorized access through a controlled access point.

**WW. Sensitive Unclassified Information (SUI)** includes unclassified information requiring protection mandated by policy or laws, such as Privacy Act Information, proprietary information, Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), and Personally Identifiable Information (PII). [Source: US-DOE: Protection of Sensitive Unclassified Information, Including Personally Identifiable Information, September 6, 2006.]

**XX. Shareware** is essentially non-commercial software created by independent software developers that is often free but sometimes requires users to pay a license fee. Often the licensing agreement does not contain terms acceptable to BPA. Shareware is also high risk software that is typically not supported by a formal organization and not well tested. It poses a significant risk to the BPA computing environment and is only permitted with Cyber Security approval. It may not be downloaded or installed without express approval.

**YY. Standards of Ethical Conduct for Government employees** are defined by 5 CFR § 2635.

	<h1>BPA MANUAL</h1>	Page 1110-5
	<h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2>	Date 01/03/07
Part: Information Management and Technology		

**ZZ. User** is any federal and/or contractor employee authorized to use BPA IT equipment.

**AAA. User ID (userid, user identification)** is one half of the authentication identifier assigned to authorized users that is required with the user's password to access computer systems that require authentication.

**BBB. Weapon** is any instrument or instrumentality used defensively for fighting, combat, and hunting such as but not limited to a semi-automatic or automatic gun (hand gun, pistol, revolver, rifle, etc.), ammunition, gun parts, sword, knife, missile, spear, bomb, explosive chemicals or parts or incendiaries.

### 1110.3 POLICY

This policy is promulgated under the authority of Title III – Information Security, Federal Information Security Management Act of 2002, Chapter 35 of Title 44, United States Code, § 3544. Federal agency responsibilities A.3.(C) “developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements.”

This policy replaces as of January 03, 2007, the existing BPA Manual Chapters 1110 and 1111 by combining them into one chapter and addressing limited personal use as a distinct subchapter for clarity.

This policy is supplemented by the Program Cyber Security Plan (PCSP) which is posted on the [Cyber Security site](#).

Questions regarding this policy should be sent to the [Cyber Security mailbox](#).

#### A. PURPOSE AND SCOPE

The purpose of this policy is to provide policy and procedures to federal and contractor employees and supervisors regarding the proper business-related use of BPA Information Technology (IT) Equipment. This policy provides notice to BPA federal and contractor employees and supervisors of the consequences for improper use of BPA IT Equipment. BPA IT Equipment represents a significant investment of BPA resources and its proper use is essential to the efficiency of the service that BPA provides.


This policy applies to all BPA federal and contractor employees. Contractor employee oversight or supervision is the responsibility of the contract company by which the contractor employee is employed. The conduct of the contractor employee in the performance of BPA business is subject to the contents of this Chapter and is managed through the contractual relationship between BPA and the contractor.

#### B. POLICY STATEMENT FOR BUSINESS-RELATED USE OF BPA IT EQUIPMENT

Except as provided by BPA Manual Chapter 1110A, BPA IT Equipment is to be used **only** by BPA federal and contractor employees who are Authorized System Users and **only** for BPA activities related to and consistent with the performance of BPA's mission and in a manner approved by this policy and consistent with Cyber Security policy or by authorized BPA personnel to determine proper use when this policy does not speak to a particular issue. This policy is intended to apply whether the work of BPA federal and contractor employees is being done within the BPA work environment or working on BPA IT Equipment from a remote location.

#### C. RESPONSIBILITY FOR PROPER AND APPROPRIATE USE OF BPA IT EQUIPMENT

BPA federal and contractor employees are responsible for knowing and understanding current BPA policy regarding the use of BPA IT Equipment, including the limits to personal use established in Chapter 1110A, and conforming their use to such policy. BPA Supervisors are responsible for ensuring that BPA federal employees, under their supervision are current in their understanding of BPA policy regarding the use of BPA

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 10px 0 0 40px;">Part: Information Management and Technology</p>	Page 1110-6
		Date 01/03/07

IT Equipment, monitoring such use, and taking appropriate actions pursuant to BPA policy to correct improper use. Contracting Officers (COs)/Contracting Officer's Technical Representatives (COTRs) are responsible for ensuring that contractor employees through their contractor manager are current in their understanding of BPA policy regarding the use of BPA IT Equipment, monitoring such use, and taking appropriate actions to correct improper use.

#### **D. CONSEQUENCES OF IMPROPER USE OF BPA IT EQUIPMENT**

BPA federal and contractor employees having authorized access to BPA IT Equipment have an obligation to understand this policy and to limit their use to the activities it allows. BPA Supervisors and Contracting Officers (COs)/Contracting Officer's Technical Representatives (COTRs) have an obligation to understand this policy and monitor the activities of BPA federal and contractor employees, respectively, sufficiently to ensure that conduct is consistent with this policy. Failure of BPA federal and contractor employees or BPA Supervisors or the CO/COTR to satisfy their obligations may subject the employee to loss of authorized system use and/or in the case of BPA federal employees to possible disciplinary action. Contractor employees may be released in accordance with the contract terms. Improper use that is suspected of violating federal laws will be reported to the appropriate law enforcement agencies.


#### **E. POLICY REGARDING ALL BPA IT EQUIPMENT INVOLVING COMPUTERS**

The following guidelines are provided to BPA federal and contractor employees and BPA Supervisors as guidance for the proper use of BPA's IT Equipment. These guidelines do not constitute the totality of rules regarding proper use of BPA's IT Equipment involving computers. For circumstances not covered by these items, see BPA IT Equipment (BPAM 1110.3.B) and the [Cyber Security Office web site](#).

1. Only BPA provided and supported IT Equipment may be connected to BPA IT Equipment. This includes connections of desktop computer systems to BPA computer network and/or connections of any peripheral device to a desktop computer that is connected to the BPA computer network.
2. Only authorized BPA IT Support Staff is permitted to modify the configuration of settings for BPA IT Equipment, including computers. BPA federal and contractor employees may, however, change desktop presentation settings (e.g., wallpaper, screen resolution, speaker volume) as provided for by BPA-approved software. In addition, BPA federal and contractor employees may make modifications under the direction of the Help Desk when troubleshooting problems.
3. Only BPA Authorized Installers are permitted to install, modify, or move BPA IT Equipment. All other persons are not authorized to install, modify or move BPA IT Equipment. Unauthorized movement, modification or installation places the BPA IT Equipment being moved and the BPA computer network in jeopardy. In addition, the location of all BPA IT Equipment must be tracked under BPA's IT Equipment asset management program.
4. No software will be installed on BPA IT Equipment without proper authorization, which must include an approved Cyber Security review. This prohibition includes downloading executable files from the Internet, downloading software purchased by BPA federal and contractor employees for personal use, downloading freeware or shareware, downloading or receiving media for demonstration of Beta versions of software provided by outside vendors or provided by other BPA federal and contractor employees. A list of currently approved software is maintained by BPA's IT Program Management (NJM) organization.

#### **F. GUIDANCE SPECIFIC TO USE OF BPA'S E-MAIL SYSTEM**


Authorized system users are encouraged to communicate with others using BPA's e-mail whenever appropriate. However, its use is subject to the following guidelines which are provided to BPA federal and

	<h1>BPA MANUAL</h1> <h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Page 1110-7
		Date 01/03/07

contractor employees and BPA Supervisors as guidance as to the proper use of BPA's e-mail system. These guidelines do not constitute the totality of rules regarding proper use of BPA's e-mail system. For circumstances not covered by these items, BPA federal and contractor employees and BPA Supervisors should consult the basic policy for use of BPA IT Equipment (BPAM 1110.3.B) and the [Cyber Security Office web site](#).

Cyber Security may disable an e-mail account that is in violation of BPA policy or that poses a threat to the BPA network. Cyber Security may be directed by the Supervisor to disable an e-mail account.

1. The BPA e-mail system and its contents, including attachments, are federal government property. As such, all messages sent with BPA's e-mail system, including those allowed by the Personal Use Allowance (BPAM Chapter 1110A), must be businesslike. Failure to use BPA's e-mail system in accordance with the above can put BPA and BPA federal and contractor employees at risk for legal liabilities, embarrassment, adverse business impacts, and other economic consequences. Upon request to Employee Relations, BPA Supervisors, have the right to review any e-mail messages, including attachments, put on the BPA e-mail system by BPA federal and contractor employees. Cyber Security and Cyber Security directed by law enforcement requests have the right to review any e-mail messages, including attachments, put on the BPA e-mail system by federal and contractor employees. BPA federal and contractor employees who have stored BPA e-mail on personally owned computing devices accept the obligation to make such e-mail available to Cyber Security.
2. BPA e-mail messages could become evidence in legal proceedings. If BPA federal and contractor employees' e-mail messages are requested under the Freedom of Information Act or litigation discovery process, BPA federal and contractor employees will be responsible for reviewing messages in their e-mail storage files and producing any responsive messages. If BPA federal and/or contractor employees store personal files not created for BPA work on BPA IT Equipment, then those files would be subject to disclosure.
3. BPA federal and contractor employees are responsible for the security of their individual BPA e-mail files and any e-mail messages they send using the BPA e-mail system. BPA federal and contractor employees should be aware that message recipients can forward the message to any number of individuals and messages may accidentally be delivered to the wrong recipient. In other words, when a BPA federal and/or contractor employee sends an e-mail message, the sending BPA federal and/or contractor employee has no control where the message may eventually go and who will read it. Care should be taken in both the preparation and sending of e-mail messages to minimize the risk that the messages will be received by unauthorized recipients. Messages sent using the BPA e-mail system and sent outside the BPA work environment will be identified as originating within BPA. Special care should be taken to ensure that such messages will only be received by intended recipients.
4. Because of the difficulty of ensuring complete security (see above), the BPA e-mail system should not be used to communicate sensitive unclassified information (SUI) without the proper safeguards authorized and provided by Cyber Security. When BPA e-mail is the only viable method of completing such communications, BPA federal and contractor employees should use extra care to ensure that the e-mail message is correctly addressed and that it will not be forwarded.
5. If the content of a BPA e-mail message possesses longer-term business value, BPA federal and contractor employees are encouraged to consider other methods of communicating the message, and if BPA e-mail is the appropriate method, to remove the e-mail message from the BPA e-mail system to a more permanent storage system. The minimum period of retention of BPA e-mail is thirty (30) days. All e-mail messages stored in the BPA e-mail system will be automatically purged (deleted) upon the

	<h1>BPA MANUAL</h1>	Page 1110-8
	<h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Date 01/03/07

expiration of that minimum period or the period established by additional policy. Some e-mail messages may constitute Official Records. Specific guidance as to the retention of Office Records is provided in the [BPA Records Manual](#).


6. Only BPA's Standard e-mail services are authorized for installation and/or use on the BPA e-mail system. BPA federal and contractor employees are not authorized to install or access any other e-mail systems (e.g., accessing an e-mail service from the Internet or third-party provider). Use of any other e-mail system or services (e.g., an e-mail service from the Internet or a web-based e-mail system via BPA Internet services) is prohibited.
7. Auto-forwarding of e-mail from the BPA's e-mail system to any other e-mail system is prohibited. Auto-forwarding of a personal e-mail into the BPA e-mail system is also prohibited.
8. Only the BPA Security and Emergency Management Office, BPA Corporate Communications, and the Office of the Chief Information Security Officer (CISO) and such BPA employees and/or organizations designated by the BPA Administrator are permitted to use the BPA e-mail system to broadcast messages. Otherwise, BPA federal and contractor employees are not permitted to use the group addressing capability of the BPA e-mail system to broadcast e-mail messages.
9. Using the BPA e-mail system for fund-raising activities other than by authorized BPA employees is prohibited.
10. Sending any passwords in an e-mail or as an attachment using the BPA e-mail system is prohibited unless the e-mail is encrypted with authorized BPA encryption software. Use of encryption must be approved by Cyber Security.
11. Sending Privacy Act of Personally Identifiable Information (PII) in an e-mail or as an attachment using the BPA e-mail system is prohibited unless the e-mail is encrypted with authorized BPA encryption software. Use of encryption must be approved by Cyber Security.
12. The BPA e-mail system may not be used for any illegal activity as defined by state or federal law, regardless of whether or not the state law applies to BPA. State laws shall include all the states in which BPA operates in which BPA is subject to by contract.
13. The BPA e-mail system may not be used to distribute chain e-mails (i.e., electronic chain letters).

### **G. GUIDANCE SPECIFIC TO USE OF BPA'S INTRA/INTERNET EQUIPMENT**

The following items are provided to BPA federal and contractor employees and BPA Supervisors as guidance to the proper use of BPA's Internet Equipment. This list of guidance items does not constitute the totality of rules regarding proper use of BPA's Internet Equipment. For circumstances not covered by these items, BPA federal and contractor employees and BPA Supervisors should consult the basic policy for use of BPA IT Equipment (BPAM 1110.3.B) and consult with their supervisors and Cyber Security.

1. Because of the continuous and dynamic risk inherent in the necessary connection between BPA Intra- and Internet and the Internet as a whole, BPA is continuously assessing, altering, adjusting and revising its policies and technologies to ensure the security of BPA's Intra- and Internet connections. Cyber Security continuously monitors Internet access and may block access to any Internet site it determines may create an unacceptable risk to BPA.
2. Upon the Supervisor's (federal employees) or the CO/COTR's (contractor employee) or law enforcement's request or as result of an intrusion detection alert or monitoring alert, Cyber Security may at its discretion review an individual's Internet usage.



	<h1>BPA MANUAL</h1>	Page 1110-9
	<h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2>	Date 01/03/07
Part: Information Management and Technology		

3. Internet posting of BPA business or security-related information, which includes BPA e-mail addresses, sensitive information or PII, for access either internally or externally is prohibited without authorization. This prohibition applies to static postings and to interactive postings, such as “blog” or “chat room” sites.
4. Because of the mechanics of some kinds of Internet searches, BPA federal and contractor employees who encounter data during authorized, business-related Internet searches that is reasonably likely to violate federal law and/or BPA policy regarding proper use of BPA IT Equipment, should report the occurrence to their BPA Supervisors and/or to the BPA Cyber Security organization and follow instructions from those authorities for preventing recurrence. If BPA federal and contractor employees are notified either electronically or otherwise that their search activities have encountered such data, they should immediately cease and desist from such search and, if necessary, consult with Cyber Security as to how their authorized search activity may be conducted without causing such encounters.
5. BPA federal and contractor employees’ personal (non-business-related) use of BPA Internet Equipment should strictly adhere to the limits set forth in BPAM Chapter 1110A.
6. The following use of BPA’s Internet connection is strictly prohibited and such use may result in disciplinary action: (1) accessing and/or downloading any form of pornography or sexually explicit, or offensive material; (2) accessing on-line gambling or gaming web sites and/or engaging in any on-line gambling or gaming.
7. The following use of BPA’s Internet connection is strictly prohibited unless previously approved and supported by Cyber Security policy: accessing and conducting financial transactions in any form.


#### **H. GUIDANCE SPECIFIC TO USE OF BPA’S REMOTE ACCESS EQUIPMENT**

The following items are provided to BPA federal and contractor employees and BPA Supervisors as guidance on to the proper use of BPA’s Remote Access Equipment. This guidance does not constitute the totality of rules regarding proper use of BPA’s Remote Access Equipment. For circumstances not covered by this guidance, BPA federal and contractor employees should consult the basic policy for use of BPA IT Equipment (BPAM 1110.3.B) and consult with their supervisors.

1. The office of the Chief Information Security Officer (CISO) manages the approval of Remote Access Service. Verification, provided by BPA Supervisors, of the business need for Remote Access Services will be required prior to granting authorization.
2. Using BPA IT Equipment via Remote Access Services for personal (non-business-related) use shall strictly adhere to the limits set forth in Chapter 1110A.
3. Authorized connections to BPA IT Equipment using Remote Access Services must be terminated as soon as the need for the use has ceased. Remaining connected to BPA IT Equipment using Remote Access Services for extended periods when there is no need for the connection ties up limited resources. Such connections, when detected will be terminated unless specifically authorized through Cyber Security.
4. Use of non-BPA IT Equipment for remote access is strictly prohibited.

#### **Chapter 1110A: Allowance for Limited Personal Use of BPA Information Technology (IT) Equipment**

##### **A. PURPOSE**

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 0;">Part: Information Management and Technology</p>	Page 1110-10
		Date 01/03/07

The purpose of this allowance and exception from BPA's otherwise business-only policy with regards to the use of BPA IT Equipment is to provide guidance to BPA federal and contractor employees and BPA Supervisors regarding the proper personal use of BPA IT Equipment. BPA IT Equipment represents a significant investment of resources by BPA and proper use is essential to the efficiency of the service which BPA was created to provide. BPA federal and contractor employees having access to BPA IT Equipment have an obligation to understand this policy and to limit their use to the activities it allows. BPA Supervisors have an obligation to understand this policy and monitor the activities of their employees sufficiently to ensure that policy limits are adhered to. Failure of BPA federal and contractor employees or BPA Supervisors to satisfy their obligations may subject them to loss of system access, disciplinary actions, and/or immediate contract termination.

This allowance does not modify the requirements of the Standards of Ethical Conduct for employees of the Executive Branch [Title 5 Code of Federal Regulations (CFR), 2635], including the employee's responsibility to protect and conserve Government property, to use it for authorized purposes only, and to use official time in an honest effort to perform official duties [5 CFR 2635.704(a) and (b)]. Nothing in BPAM Chapter 1110A pertains to or restricts use of Government property by an employee to carry out his or her official duties and responsibilities in furtherance of the mission of BPA.

### **B. POLICY STATEMENT RELATED TO PERSONAL USE OF BPA IT EQUIPMENT**

BPA IT Equipment is to be used only for supervisor-authorized activities related to and consistent with the performance of BPA's mission, subject to the limited personal use allowance provided below.

### **C. LIMITED PERSONAL USE ALLOWANCE**

Personal use of designated BPA IT Equipment is allowed within the limits and prohibitions specified in this policy. This allowance does not grant or create an inherent right to use Government resources, and one should not be inferred.

Any personal use, even if ostensibly allowed by this policy, may be further limited or revoked at any time by BPA Supervisors or Cyber Security when circumstances warrant such action.


### **D. RESPONSIBILITY FOR PROPER AND APPROPRIATE PERSONAL USE OF BPA IT EQUIPMENT**

BPA federal and contractor employees are responsible for knowing and understanding current BPA policy regarding the use of BPA IT Equipment, including the limits to the allowance for limited personal use established by BPAM Chapter 1110A, and conforming their use to such policy. BPA Supervisors are responsible for

1. ensuring that BPA federal and contractor employees under their supervision and/or direction remain continuously current in their understanding of BPA policy regarding the use of BPA IT Equipment;
2. monitoring potential misuse as appropriate in conjunction with Cyber Security and Employee Relations; and
3. taking appropriate actions pursuant to BPA policy to correct inappropriate use when inappropriate use is observed or reported.

### **E. CONSEQUENCES OF IMPROPER PERSONAL USE OF BPA IT EQUIPMENT**

Failure of BPA federal and contractor employees or BPA Supervisors to satisfy their responsibility for proper and appropriate personal use of BPA IT Equipment may subject them to loss of system access and/or possible disciplinary actions or immediate contract termination.

	<h1>BPA MANUAL</h1>	Page 1110-11
	<h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2>	Date 01/03/07
Part: Information Management and Technology		

### F. APPLICATION OF NATIONAL SECURITY LEVELS TO LIMITED PERSONAL USE ALLOWANCE


The limited personal use allowance stated in BPAM Chapter 1110A.C applies to all BPA IT Equipment only when the national security level has been designated as Green. The allowance is further limited when the national security levels are other than Green as follows:

1. When the national security level has been designated as Orange or Red, there shall be no personal use of BPA IT Equipment unless otherwise authorized by Cyber Security.
2. When the national security level has been designated as Yellow, personal use allowance shall be permitted on BPA IT Equipment. However, web site and e-mail blocking may increase as the result of DOE, Homeland Security and other official advisories. Should increased web site and e-mail blocking become necessary, Cyber Security shall use official communication channels to notify the workforce in general provided such advisories are not sensitive or classified.
3. When the national security level has been designated as Green or Blue, the personal use policy shall be permitted on BPA IT Equipment. However, web site and e-mail blocking may increase as the result of DOE, Homeland Security and other official advisories. Should increased web site and e-mail blocking become necessary, Cyber Security shall use official communication channels to notify the workforce in general provided such advisories are not sensitive or classified..
4. In situations, where National Security Levels are not modified but there is a credible threat reported by law enforcement, Homeland Security, or the DOE Inspector General or DOE incident response (CIAC) or other official sources, Cyber Security may revoke limited personal use authorization throughout BPA until the threat has been cleared. Prior and subsequent to revocation or the threat being cleared, Cyber Security shall notify the workforce through official BPA channels.


### G. SPECIFIC PROHIBITIONS

In all cases, personal use of BPA IT Equipment on duty time is prohibited. That is, personal use of BPA IT Equipment is only permitted before the workday begins, after the workday ends or during lunch time. The following specific restrictions apply to BPA federal and contractor employees' personal use of BPA IT Equipment:

1. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment for any personal use that interferes with employees' official duties or reflects badly on the conduct of the federal service (this prohibition includes the use of language that would reflect badly on the federal service in otherwise allowed personal use instances). The prohibition especially prohibits gambling and the viewing or correspondence about and/or trading or procurement of weapons of any kind.
2. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment for any personal use that has been made unlawful by federal, state or local law (whether or not such state or local law governs the conduct of BPA as a federal agency).
3. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment to maintain or support a personal private business or to assist family, friends or other persons in such activities.
4. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that violates the Standards of Ethical Conduct for Government employees.

 <p><b>BONNEVILLE</b> POWER ADMINISTRATION</p>	<h1>BPA MANUAL</h1> <h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Page 1110-12
		Date 01/03/07

5. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment in a way that expressly or impliedly represents that BPA or the federal government has sanctioned or endorsed the specific purpose of the personal use.
6. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that communicates an express or implied threat or violates BPA's Harassment-Free Workplace Policy.
7. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that includes communication of material (language and/or pictures) that a reasonable person would find offensive (e.g., hate speech, material that ridicules others on the basis of race, gender, color, religion, disability, national origin, sexual orientation, educational and/or economic level).
8. BPA federal and contractor employees are specifically prohibited from using BPA IT Equipment in any personal use that creates a risk to BPA IT Equipment systems (e.g., when such use creates or increases the possibility of threats to BPA IT Equipment by malicious software [Malware]).
9. BPA federal and contractor employees are specifically prohibited from personal use of Operational and Control IT Equipment such as Instrument Controllers (ICs) under any circumstances.
10. While offsite, BPA federal and contractor employees are not permitted to use BPA IT Equipment to connect "directly" to the Internet using a modem (dial up), wireless or wired connection. All connections must be made to the BPA administrative network using VPN software or authorized software. A violation may result in the revocation of remote access privileges.
11. BPA federal and contractor employees are specifically prohibited from removing BPA IT Equipment from the BPA work environment in order to use such equipment for personal use. However, when there is a BPA business requirement to relocate BPA IT Equipment, such relocation may be done through the BPA established processes.
12. BPA federal and contractor employees are specifically prohibited from making purchases of any product for personal use using BPA IT Internet Equipment.
13. BPA federal and contractor employees are specifically prohibited from personal use of any BPA IT Equipment that is designated for classified use under the National Security Act.
14. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment that imposes more than minimal additional expense to BPA unless authorized by BPA.
15. BPA federal and contractor employees are specifically prohibited from any personal use of BPA IT Equipment that gives the impression that the user is acting in an official capacity.
16. BPA federal and contractor employees are specifically prohibited from any personal use that requires the downloading (i.e., copying) from any non-BPA IT or BPA IT Equipment of large files (greater than five megabytes) such as documents, attachments, motion or still images, digital audio files, and data into BPA IT Equipment.
17. BPA federal and contractor employees are specifically prohibited from any personal use of a program or Internet site that provides continuous data streams to BPA IT Equipment, even if such streams are not stored as files within BPA IT Equipment (e.g., continuous stock quotes, radio broadcasts, news headlines, weather, etc.).
18. BPA federal and contractor employees are specifically prohibited from creating, downloading, viewing, storing, copying or transmitting sexually explicit or sexually oriented materials using BPA IT Equipment.

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 10px 0 0 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 10px 0 0 0;">Part: Information Management and Technology</p>	Page 1110-13
		Date 01/03/07

19. BPA federal and contractor employees are specifically prohibited from participation in fundraising for any entity or activity other than authorized activity related to the Combined federal Campaign or Associates Functions using BPA IT Equipment.
20. BPA federal and contractor employees are specifically prohibited from participation in any political activity using BPA IT Equipment.
21. BPA federal and contractor employees are specifically prohibited from modification of BPA IT Equipment in any way to facilitate personal or BPA official business use.
22. BPA federal and contractor employees are specifically prohibited from installation of any non-BPA owned software or hardware devices on BPA IT Equipment to facilitate personal use.
23. BPA federal and contractor employees are specifically prohibited from any frequent personal use that may cause congestion, delay, or disruption of service to any BPA IT Equipment, including greeting cards, audio, and streaming video and audio, etc., unless authorized by Cyber Security.
24. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment that involves unauthorized acquisition, use, reproduction, transmission, or distribution of controlled information (e.g., computer software and data; classified, business sensitive, or other nonpublic data; proprietary data; export controlled software or data; or any information in violation of the Privacy Act, copyright, trademark, or other intellectual property rights beyond fair use).
25. BPA federal and contractor employees are specifically prohibited from personal use of BPA IT Equipment that involves gaining authorized access to internal or external systems or networks.

#### **H. NO PRIVACY EXPECTATION FOR PERSONAL USE**


BPA federal and contractor employees should understand that there is no right and should be no expectation of privacy. BPA federal and contractor employees' use of BPA IT Equipment is always subject to supervision and such supervision may include supervisory review, including active monitoring through the use of monitoring tools, of BPA federal and contractor employees' use of BPA IT Equipment and the content of materials stored within BPA IT Equipment. Personal use of BPA IT Equipment by BPA federal and contractor employees implies consent by such employees to such review. BPA federal and contractor employees who wish their personal use activities to be private should not use BPA IT Equipment for personal use.

BPA federal and contractor employees should further understand that the content, whether personal or work related, stored within BPA IT Equipment is the property of BPA and may be disclosed in response to a valid subpoena, warrant, court order (including litigation discovery request), Freedom of Information Act (5 USC 552) request, or other authorized direction (e.g., BPA federal and contractor employees' supervisor, Cyber Security, Inspector General, etc.).

#### **I. GUIDANCE FOR ALLOWED PERSONAL USE**

The following examples are provided solely for the purpose of guidance for BPA federal and contractor employees and BPA Supervisors to understand what may be allowed as personal use of BPA IT Equipment. BPA federal and contractor employees and BPA Supervisors should not rely on these examples as specific grants of authority for the uses described. If BPA federal and contractor employees or BPA Supervisors are in doubt about whether a specific personal use is or is not allowed by this policy, they should always seek specific authority from their supervisors and/or Cyber Security.


##### **Examples:**

	<h1 style="margin: 0;">BPA MANUAL</h1> <h2 style="margin: 0;">Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p style="margin: 0;">Part: Information Management and Technology</p>	Page 1110-14
		Date 01/03/07

1. Occasionally during work and non-work hours using e-mail or telephone, including voice mail, to keep in touch with family members/or significant others regarding work and/or school schedules (e.g., BPA federal and contractor employees calls or e-mails spouse to inform spouse she will be required to work overtime; BPA federal and contractor employee calls or e-mails dependant's school to confirm time of parent-teacher meeting, etc.). Occasional use is less than ten minutes during duty time unless otherwise authorized by a supervisor. Occasional use in this context are times outside of the non-work time definition.
2. Using e-mail or telephone to check on status of bank, credit union or TSP accounts under the non-work time definition not to exceed two (2) continuous hours in any non-work period.
3. Preparing and storing current resume and related materials on the local hard drive only under the non-work time definition with no time limit.
4. Accessing public library, newspaper and similar publicly available data that does not include downloading (copying) significant amounts of data or printing numerous or large documents on BPA printers under the non-work time definition not to exceed two (2) continuous hours in any non-work period. Any downloading of data must be to the local hard drive and must not occupy more than fifteen (15) percent of the available hard drive storage space.
5. Conducting research regarding personal travel arrangements or consumer matters (e.g., Kelly Blue Book information) on web sites under the non-work time definition not to exceed two (2) continuous hours in any non-work period.
6. Checking current or predicted weather on web sites under the non-work time definition not to exceed two (2) continuous hours in any non-work period.
7. Personal electronic images may be stored on the local hard drive but not on the H: drive or any other network drive, provided such photographs do not occupy more than fifteen (15) percent of the total data storage on the local hard drive, have been scanned for malicious software and are not in violation of any federal or state laws, regulations, policies or DOE Orders.
8. All BPA federal and contractor employees are permitted to use BPA IT Equipment for reasonable personal use via Remote Access Services (Dial-up, Internet, Wireless) on official travel status and in conjunction with a valid telecommuting agreement. The user must access the Internet through an authorized BPA access point using either the VPN software for wired and wireless connections or the authorized software for dial-up. Failure to follow this process may result in the revocation of remote access privileges.

#### 1110.4 RESPONSIBILITIES

**A. Federal and contractor Employees** are responsible for the knowledge and the understanding of current BPA policy regarding the use of BPA IT equipment, including the limits of personal use, established in Cyber Security Chapter 1110.A, and are to conform to the use of such policy. BPA federal and contractor employees, who have authorized access to BPA IT equipment, have an obligation to understand this policy and to limit their use to the activities as allowed. Failure of BPA **federal and contractor employees** or BPA supervisors or CO/COTRs to satisfy their obligations, may subject the employee to loss of authorized system use and/or in the case of BPA federal employees to possible disciplinary action.

	<h1>BPA MANUAL</h1>	Page 1110-15
	<h2>Chapter 1110: Business Use of BPA Information Technology Services Policy</h2> <p>Part: Information Management and Technology</p>	Date 01/03/07

- B. **Supervisors** are responsible for ensuring that BPA **federal employees**, under their supervision are current in their understanding of BPA policy regarding the use of BPA IT equipment, monitoring such use, and taking appropriate actions pursuant to BPA policy to correct improper use. BPA supervisors have an obligation to understand this policy and monitor the activities of BPA federal employees sufficiently to ensure that their conduct is consistent with this policy.
- C. **Contracting Officers (CO) and Contracting Officer Technical Representatives (COTRs)** are responsible for ensuring that **contractor employees** working through their contractor manager, are kept current in their understanding of BPA policy regarding the use of BPA IT equipment, monitoring such use, and taking appropriate actions to correct improper (inappropriate) use. BPA Contracting Officers (COs)/Contracting Officer Technical Representatives (COTRs) have an obligation to understand this policy and monitor the activities of **contractor employees** sufficiently to ensure that their conduct is consistent with this policy. **Contractor employees** who do not comply with the policy may be released in accordance with the contract terms.
- D. **Contractors** are responsible for oversight or supervision of the **contractor employees** and ensuring adherence to these policies.

### 1110.5 PROCEDURES

No information in this section.

### 1110.6 REFERENCES

- A. **Pub. L. No. 93-579, Title 5 U.S.C. § 552a**, Privacy Act of 1974 (2000)
- B. **Pub. L. No. 107-347, Title III, 44 U.S.C. § 3544 (a)(3)(C)**, Information Security, Federal Information Security Management Act of 2002
- C. **5 CFR § 2635**, Standards of Ethical Conduct for Employees of the Executive Branch
- D. **5 CFR § 2635.704(a) and (b)**, Standards of Ethical Conduct for Employees of the Executive Branch
- E. **US-DOE: Protection of Sensitive Unclassified Information, Including Personally Identifiable Information**, September 6, 2006
- F. **BPA Manual Chapter 400/700A, Appendix A**, BPA's Harassment-Free Workplace Policy
- G. **BPA Program Cyber Security Plan (PCSP)**
- H. **Cyber Security Policy BPA-20060809-001**, Personally Identifiable Information (PII)