BPA Policy 470-8

Business Use of BPA IT Services and Equipment

Table of Contents

1. Purpose & Background

The purpose of this policy is to establish requirements, assign responsibilities, and provide guidance for business-related use of Bonneville Power Administration (BPA) Information Technology (IT) products and services.

BPA's Information Technology organization's overarching mission is to build sustainable partnerships with our users to create IT solutions for business success, thereby enabling BPA to achieve its mission in the most safe, secure, and cost-conscious manner. This mission is reliant upon BPA's ability to manage IT assets as efficiently as possible, while providing enough flexibility for personnel to accomplish their work requirements, and ensuring that IT assets adhere to the standards defined by the National Institute of Standards and Technology (NIST), Federal and State regulations, laws, memorandums, and directives, as well as BPA's Cyber Security Program Plan (CSPP) and the Chief Information Officer (CIO).

BPA IT products and services represent a significant investment of BPA resources and their use is essential to the efficiency of the service that BPA provides. The misuse of BPA IT products and services poses significant risks to the mission and business of BPA.

2. Policy Owner

The BPA Chief Information Officer (CIO) has overall responsibility for this policy.

3. Applicability

This policy applies to the use of all BPA IT services and equipment.

This policy applies whether the work is performed within the BPA work environment or from a remote location.

4. Terms and Definitions

A. **Authorized System Users**: BPA personnel who are:

1. validated to meet all pre-requisites, such as background checks, training, and physical access, as detailed by the relevant system, and
2. granted access to said system.

B. **BPA Authorized Installers**: Designated personnel who are authorized to install, update and remove BPA licensed software on government-furnished end-user devices (typically desktop, laptop, tablet, smart phone, or virtual machine). In addition, BPA Authorized Installers are authorized to install, modify and move BPA IT equipment. This designation is granted by the System Owner (SO) of the related BPA IT equipment.

C. **BPA IT Equipment**: Includes but is not limited to any BPA-owned or leased device that can be attached or connected to, or interact with, any network, service, or application operated by, or on behalf of, BPA, including any IP-addressable equipment or devices. BPA IT equipment includes, but is not limited to, desktop computers, laptops, tablets, thin clients, firmware, software, shareware, freeware, desk telephones, digital cameras, cell phones, smart phones, facsimile machines, copiers, printers, scanners, multifunction devices (e.g., combined copier, printer, and scanner), servers, fixed or portable storage devices (e.g., USB flash drives), network routers and switches, and peripheral devices (e.g., monitors, keyboards, PIV readers). BPA IT equipment may be represented in physical, on-premises-virtual, and/or cloud-virtual (e.g., cloud-based IT services such as Desktop-as-a-Service, Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service) forms.

D. **BPA IT Services**: Any service performed by BPA IT personnel in relation to BPA IT equipment. Examples include trouble-shooting, repair, training, planning, installation and configuration, managing, etc.

E. **Dual Use IT Equipment**: IT equipment that is used as both administrative IT equipment and Transmission grid operational and control IT equipment.

F. **Information Technology (Title 40 US Code, Section 11101)**: With respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use –

   a) of that equipment; or

   b) of that equipment to a significant extent in the performance of a service or the furnishing of a product

   It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources. All IP-addressable equipment or devices are included in this category.

G. **Personal Use**: Use of BPA IT equipment for non-BPA business.

H. **Peripheral Devices**: Computer devices, such as a cell phone, webcam, flash drive or printer, that is not part of the essential computer (e.g., the memory and microprocessor). Peripheral devices can be external or internal. Examples of external peripheral devices include a mouse, keyboard, printer, webcam, etc. Examples of internal peripheral devices, often referred to as integrated peripherals, include network card, e-card reader, cd/dvd drives, etc.

5. Policy

A. **Business Use of BPA IT Services**: BPA IT services are to be used:

1. Only by Authorized System Users.
2. Only for BPA activities related to, and consistent with, the performance of BPA's mission, or for limited personal use of BPA IT services as defined in BPA Policy 470-6.
3. Only in a manner approved by this policy and consistent with other Cyber Security policy, or by BPA personnel authorized to determine proper use when this policy does not address a particular issue.

B. **Business Use of BPA IT Equipment**:

1. BPA IT equipment is to be used:
   a) Only by Authorized System Users.
   b) Only for BPA activities related to, and consistent with, the performance of BPA's mission, or for limited personal use of BPA IT equipment as defined in BPA Policy 470-6.
   c) Only in a manner approved by this policy and consistent with other Cyber Security policy, or by BPA personnel authorized to determine proper use when this policy does not address a particular issue.
2. All information stored within BPA IT equipment is the property of BPA and may be disclosed in response to a valid subpoena, warrant, court order, litigation discovery request, Freedom of Information Act (5 USC 552) request, or for other legitimate business reasons.
3. Only BPA IT equipment may be connected to BPA IT equipment when working at a BPA facility.
4. Only the following BPA IT equipment may be taken off-site to support the performance of an employee's official duties, and any limited personal use shall be incidental to the official use and comply with BPA Policy 470-6:
   a) BPA-Issued:
      i) Cell phones
      ii) Smart phones
      iii) Laptops
      iv) Tablets
      v) Notebook computers
5. Specific non-BPA peripheral devices, which do not store data or require installation of special drivers or software to function, may be connected to BPA IT equipment

while off-site if the equipment assists with the performance of official duties. These include:

a) Keyboards

b) Monitors

c) Mice

d) Webcams

e) Universal docking stations

f) Bluetooth headsets

6. The following peripheral devices must not be connected to BPA IT equipment at any time:

   a) Non-BPA-Issued:

      i) Cell phones

      ii) Smart phones

      iii) External hard drives

      iv) DVD-ROM drives

      v) Printers

      vi) Scanners

      vii) USB thumb/flash drives

      viii) Smart TVs (unless not connected to any network)

7. Only authorized BPA IT support staff are authorized to modify BPA IT equipment configuration settings.

   a) At the direction, and under the supervision, of the IT Support Desk or Client Support, Authorized System Users may be enabled and directed to make these modifications.

   b) Authorized System Users may have permissions to modify non-security related configuration settings. An example of these would be desktop presentation settings (e.g., wallpaper, screen resolution, speaker volume) as provided for by BPA-approved software.

8. Only BPA Authorized Installers are authorized to install or modify BPA IT equipment.

9. Only BPA Authorized Installers are authorized to move BPA IT equipment that is not designed for mobile use, such as desktop computer towers, printers, servers, network switches, or monitors.

a) BPA IT equipment designed for mobile use include, but are not limited to, laptops, tablets, notebook computers, cell phones, and smart phones.

b) Unauthorized movement, modification, or installation of BPA IT equipment places it, and the BPA computer networks they connect to, in jeopardy.

10. The physical location of all property tagged BPA IT equipment must be accounted at least once annually under BPA's IT equipment asset management program.

11. All software installed on BPA IT equipment must be approved by the BPA Office of Cyber Security.

    a) A list of currently approved software is maintained by BPA's End User Services organization.

    b) The IT Policy Library contains information on how to get software titles onto the Approved Software List (See ASL Policy).

    c) Freeware and Shareware are only permitted after approval of the CIO.

12. Use of unauthorized or unapproved software on BPA IT equipment is strictly prohibited. This prohibition includes, but is not limited to, the following:

    a) Executable files (commonly known as programs) from the internet

    b) Software purchased by anyone for personal use

    c) Freeware or Shareware (without CIO approval)

    d) Beta versions of software provided by outside vendors (BETA software is a test version not officially released for production sale or use by the author)

    e) Software provided by anyone not authorized by BPA to do so

13. Dual use IT equipment is strictly prohibited on BPA networks.

    a) BPA IT equipment may be configured and used on Transmission grid and on BPA business administrative networks. BPA IT equipment used on Transmission grid operational and control or administrative networks must not be connected to any non-BPA networks under any circumstances.

    b) Violation of this prohibition places BPA systems and networks in jeopardy.

C. **Limited Personal Use of IT Services and Equipment**: Personal use of designated BPA IT services and BPA IT equipment is allowed within the limits and prohibitions specified in this policy. This allowance does not grant, nor create, a right to use any government resources, including IT services and equipment. Any personal use, even if allowed by this policy, may be further limited or revoked at any time by an employee's supervisor or Cyber Security.

1. **Specific Allowances and Prohibitions for Limited Personal Use**: Authorized System Users have certain allowances for, and prohibitions from, using BPA IT equipment.

These can be found in BPA Policy 470-6 Limited Personal Use of BPA IT Services and Equipment.

2. **No privacy expectation**: There is no right to privacy related to the use of BPA IT services or equipment. Communications using, or information captured by or stored on, BPA IT equipment are not private and are subject to routine monitoring, interception, and search, and may be disclosed or used for any authorized purpose. At any time, authorized personnel may inspect and seize any information stored on BPA IT equipment.
3. **Application of national threat levels to limited personal use allowance**: The limited personal use allowance may be modified by BPA's Office of Cyber Security due to changes in the national threat level, or other credible threats. Should additional limits, such as web site or email blocking, or complete revocation of limited personal use, become necessary, BPA's Office of Cyber Security shall use official communication channels to notify the workforce in general.

D. **Business Use of BPA Mobile Equipment**: Business use of BPA mobile equipment is specified in BPA Policy 470-7 Mobile Technology Management.

E. **Business Use of BPA's Email System**: BPA's email system is an important tool used to carry out BPA's mission. All employees are required to use it in a professional manner and are prohibited from sending emails or attachments that violate the BPA Code of Conduct. Failure to use BPA's email system in accordance with policy can put BPA at risk for legal liabilities, adverse business impacts, and/or reputational harm.

1. The BPA email system and its contents, including attachments, are federal government property and may qualify as a government record.
    a. All messages sent or received using BPA's email system, including those allowed by BPA's limited use policy, must be business-appropriate in nature.
2. There is no right to privacy related to the use of BPA's email system. Emails sent, received or stored on the BPA system are subject to routine monitoring, interception, and search. Authorized personnel may inspect, seize, and/or disclose email content for any legitimate business purpose at any time.
3. The BPA Office of Cyber Security is authorized to review any email messages, including attachments, entered into, or received by, the BPA email system.
    a. Storing BPA business related emails on personal devices is prohibited. BPA emails stored on personal devices are subject to recovery by BPA or other authorized federal official. Such emails shall be produced immediately upon request from BPA's Office of Cyber Security or appropriate federal official.

4. BPA email messages are subject to the Freedom of Information Act and other information disclosure obligations.

    a. If requested, employees are responsible for reviewing all stored emails and producing any responsive materials.

    b. BPA may use automated discovery software (e.g., eDiscovery) to identify relevant emails.

    c. Any emails stored in a BPA system are subject to disclosure.

5. Email accounts that are in violation of BPA policy or that pose a threat to the BPA networks may be disabled. Appropriate management officials and BPA's Office of Cyber Security are authorized to disable an email account.

6. **Use of other Email Systems**: Only BPA's email services are authorized for installation on BPA IT equipment and to conduct official business. See BPA Policy 236-260 Email Management for additional details.

    a. Authorized System Users are prohibited from installing, or accessing, any other email systems (e.g., accessing an email service from the internet or third-party provider).

    b. BPA prohibits the use of personal/non-BPA email accounts to conduct official business. This includes all email components such as messages, tasks, calendar events, etc.

    c. Auto-forwarding of email from the BPA email system to any other email system is prohibited.

    d. Auto-forwarding of a personal email into the BPA email system is prohibited.

7. **Prohibited use of BPA Email System**:

    a. Using the BPA email system for charitable fund-raising activities, except the Combined Federal Campaign (CFC) or other federally authorized activities.

    b. Sending unprotected passwords for password-protected or encrypted information in the same email that contains the protected information, or as an attachment.

        i. It is an acceptable practice to send an unencrypted clear-text password in a separate email for information that is encrypted.

        ii. Encrypted information must be encrypted with BPA approved encryption software or following the guidance provided in BPA Procedure 433-1-2.

c. Sending Privacy Act information or sensitive Personally Identifiable Information (PII) in an email or as an attachment using the BPA email system is prohibited unless the email is encrypted with BPA approved encryption software.

d. The BPA email system may not be used for any illegal activity as defined by state or federal law.

e. The BPA email system may not be used to distribute chain emails (emails that are designed to be constantly forwarded) that are not for conducting BPA business.

F. **Business Use of BPA's Intranet and Internet equipment**: Due to the continuous and dynamic risk inherent in the necessary connection between BPA intranet and internet, and the internet as a whole, BPA is continuously assessing, altering, adjusting and revising its standards and technologies to ensure the security of BPA's intranet and internet connections.

1. BPA's Office of Cyber Security may block access to any internet site it determines may create an unacceptable risk to BPA.

2. BPA's Office of Cyber Security may review internet usage for any legitimate business reason.

3. Employees who encounter information that, by its existence or transmission, is reasonably likely to violate federal or state law, or BPA policy, must report the occurrence to their BPA supervisors, the BPA Office of Cyber Security, or both.

   a. If Users are notified, either electronically or otherwise, that their internet activities have encountered such information, they should immediately cease and desist from such activities and, if necessary, consult with the BPA Office of Cyber Security as to how their authorized activity may be conducted without causing such encounters.

4. Unless specifically granted written exception by the BPA Office of Cyber Security, access to any internet-based services from BPA IT equipment must be conducted using a secure connection to BPA's administrative network. Secure connections include:

   a. Directly on the BPA administrative network.

   b. BPA-provided VPN.

   c. myPC remote access.

5. Authorized System Users' personal use of BPA internet equipment must strictly adhere to the limits set forth in BPA Policy 470-6 Limited Personal Use of BPA IT Services and Equipment.

6. **Prohibited use of BPA's Intranet and Internet equipment:**

    a. The act of posting, publishing, or making generally available to the internet, sensitive BPA business or security-related information, including BPA email addresses and sensitive personnally identifiable information (PII), for general access either internally or externally, is prohibited without written prior authorization.

        i. This prohibition applies to all postings, including, but not limited to, static postings and interactive postings, such as "blog" or "chat room" sites.

        ii. See BPA Policy 472-1 Use of Social Media and Web 2.0 Tools for additional information on the use of the internet.

    b. Accessing or downloading any form of pornography or sexually explicit or offensive material.

    c. Accessing on-line gambling or gaming websites or engaging in any on-line gambling or gaming.

    d. Personal financial transactions conducted using BPA internet services without previous written approval by the BPA Office of Cyber Security.

        i. Use of BPA authorized micro purchase program (P-Card) via BPA internet services for legitimate business reasons is approved.

G. **Business use of BPA's telephone equipment**: BPA's telephone system and supporting equipment is an important tool used to carry out BPA's mission. All usage is required to be in a professional manner.

1. Use of long distance dervices for telephone calls:

    a) Official outgoing long distance telephone calls must be placed using BPA-issued telephonic devices (e.g. desk phone, soft phone or BPA-issued smartphone).

    b) Forwarding of desk phones to cellular phones must use the procedures provided by Information Technology's Voice & Video Services organization. These are located on the SharePoint site, and can be obtained through the BPA Operator.

    c) Do not authorize or accept incoming collect calls unless required for official BPA business purposes.

6. Policy Exceptions

There are no exceptions to this policy.

7. Responsibilities

A. The BPA Chief Information Officer (CIO)

1. Sponsors and administers this policy including: overseeing periodic review, ensuring consistency with BPA strategic and operational plans, and meeting regulatory requirements.
2. Reports any significant violations of this policy, or the standards and operations procedures referenced in this policy, to the BPA executive governance body.

B. Authorized System Users

1. Are required to be familiar with current BPA policy regarding the use of BPA IT services and equipment, including the limits of personal use established in BPA Policy 470-6 Limited Personal Use of BPA IT Services and Equipment, and conforming their use of these BPA resources to policy requirements.

C. BPA Supervisors and Managers

1. Are responsible for ensuring that their organizations are current in their understanding of BPA policy regarding the use of BPA IT services and equipment.
2. Have an obligation to understand this policy and observe the activities of BPA Federal employees sufficiently to ensure that their conduct is consistent with this policy.

D. Contracting Officer Representatives (CORs) and Field Inspectors

1. Are responsible for ensuring that contracts providing companies with access to BPA IT services or equipment include a clause requiring adherence to this policy.
2. Have an obligation to understand this policy and observe the activities of contractor employees sufficiently to ensure that their conduct is consistent with this policy.

8. Standards & Procedures

None at this time.

9. Performance & Monitoring

On a continuous basis, a delegate assigned by the CIO shall report to the CIO:

A. Any significant violations of this policy. These violations shall also be reported to the BPA executive governance body.

10. Authorities & References

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."

A. BPA Policy 473-2 Information Technology Policies
B. BPA Policy 470-6 Limited Personal Use of BPA IT Services
C. BPA Policy 470-7 Mobile Technology Management
D. BPA Policy 472-1 Use of Social Media and Web 2.0 Tools
E. Pub. L. No. 93-579, Title 5 U.S.C. § 552a, Privacy Act of 1974 (2000)
F. Pub. L. No. 107-347, Title III, 44 U.S.C. § 3544 (a)(3)(C), Information Security, Federal Information Security Management Act of 2002
G. Title 40 U.S. Code Subtitle III Information Technology Management
H. 5 CFR § Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch
I. US-DOE: Protection of Sensitive Unclassified Information, Including Personally Identifiable Information, September 6, 2006
J. BPA Cyber Security Program Plan (CSPP)
K. BPA Policy 470-3 Protection of Personally Identifiable Information Within the BPA Application Portfolio
L. BPA Policy 433-1 Information Security
M. DOE O 206.1 Department of Energy Privacy Program

11. Review

This policy shall be reviewed by the policy owner at least every three years for relevant purpose, content, currency, effectiveness, and metrics.

12. Revision History

This chart contains a history of the revisions and reviews made to this document.

Version Number	Issue Date	Brief Description of Change or Review
1.0	4 June 2024	Initial Publication of Policy