BONNEVILLE POWER ADMINISTRATION

BPA Policy 470-7

Mobile Technology Management

Table of Contents

1. Purpose & Background

The purpose of this policy is to establish requirements, assign responsibilities, and provide guidance for mobile technology management and employee use of both Government Furnished Equipment (GFE) and non-GFE mobile devices for conducting official Bonneville Power Administration (BPA) business.

BPA recognizes the value and convenience of providing remote access to internal BPA systems from both GFE and non-GFE mobile devices.

BPA staff are provided with BPA-owned mobile devices based on operational needs and job responsibilities. These devices may take the form of:

- Cellular Phones
- Smartphones
- Tablets
- Laptop Devices

Use of non-GFE mobile devices for access to BPA IT services and equipment assets provides workplace flexibility, and is granted to BPA staff and visitors through approval of management. Remote access in a telework situation must be performed in accordance with HR Directive 410-06-03 Telework and Remote Work Program.

In all cases, access to BPA IT services and equipment assets is expressly granted to accomplish official BPA business. BPA Policy 470-6, Limited Personal Use of BPA IT Services and Equipment, is applicable to all uses granted such access.

This policy supports, and is consistent with, DOE O 203.2, Mobile Technology Management, adhering to all requirements, responsibilities, and guidelines except for deviations or clarifications specifically identified within this policy.

2. Policy Owner

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

3. Applicability

This policy applies to the use of mobile devices accessing, connecting to, or interacting with, BPA IT services and equipment.

4. Terms & Definitions

A) **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.

B) **Corporate Wireless Network Access:** The ability to connect a BPA-issued device with IEEE 802.11 compliant wireless capabilities to a BPA-owned and operated wireless local area network (WLAN or Wi-Fi) through wireless access points (WAP) for the purposes of accessing BPA corporate network resources.

C) **Guest Wireless Network Access:** The ability to connect a non-GFE device with IEEE 802.11 compliant wireless capabilities to a BPA-owned and operated wireless local area network (WLAN or Wi-Fi) through wireless access points (WAP), for the purposes of accessing the public Internet only. Non-GFE wireless devices with access to the BPA guest wireless network will have no direct access to the internal BPA corporate networks or records.

D) **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.

E) **Remote Access to Internal BPA Systems From a Non-BPA Device:** The ability to access a BPA Virtual Desktop Infrastructure (VDI) (e.g., myPC.bpa.gov) session, using a non-BPA device running a client virtualized desktop connector (e.g., Citrix Receiver free software application provided by Citrix Systems, Inc.), from a remote location.

5. Policy

All uses identified in section 3 (Applicability) of this policy, must adhere to all requirements, responsibilities, and guidelines provided within DOE O 203.2, Mobile Technology Management, with the following deviations or clarifications:

A) Mobile Device Management (MDM) solutions, DOE O 203.2.4.b.3, is augmented as follows:

a. An automated MDM solution for device monitoring and control for devices that store sensitive BPA information must be implemented.

b. The MDM solution must provide at least the following capabilities:

i. Enable identity verification and authentication requirements for access to BPA data and systems via mobile devices.

ii. Enable data encryption and sanitization (device erasing).

iii. Employ patch and configuration management strategies.

iv. Employ monitoring for device breaches, including additions of applications not provided through the MDM solution.

B) Technology Solutions, DOE O 203.2.4.j, is augmented as follows:

a. A BPA guest wireless network is provided that enables access to the internet, but not to internal BPA IT services and equipment.

i. Guest Wireless Network Access is limited to non-GFE devices for sponsored guests of BPA.

ii. Non-GFE devices are limited to internet access only, and are strictly prohibited from using Corporate Wireless Network Access.

iii. GFE devices with IEEE 802.11 compliant wireless capabilities are prohibited from using Guest Wireless Network Access.

b. A BPA corporate wireless network is provided that enables direct access to internal BPA IT services and equipment.

i. Corporate Wireless Network Access is limited to GFE devices only.

ii. Non-GFE devices are prohibited from using Corporate Wireless Network Access.

c. In relation to BPA's Virtual Desktop Infrastructure (VDI), designated as myPC:

i. Non-GFE devices must use BPA's myPC remote access solution to access any BPA corporate network.

ii. Remote access to myPC is limited to currently approved client virtualized desktop connectors.

d. Non-GFE mobile devices are prohibited from directly connecting to any BPA corporate network.

e. BPA will not port or transfer an existing BPA smart phone or cell phone number to a non-GFE mobile device.

f. Access to BPA email, calendar, and contact services outside of BPA's VDI is restricted to GFE devices.

i. Non-GFE mobile devices are prohibited from accessing BPA email, calendar, and contact services except through BPA's VDI.

g. Non-GFE devices are prohibited from directly accessing any BPA corporate network, including, but not limited to, the use of a VPN or direct connection.

C) Reimbursement, DOE O 203.2.4.e, is amended as follows:

BPA will not reimburse for any cost associated with the usage of non-GFE regardless of the reason for the usage. This includes but is not limited to: charges resulting from text messages, data plan surcharges, phone calls, navigation, application purchases, handset replacement and insurance plans, early termination fees, mobile carrier support, accessories, purchase or acquisition of a personally-owned device, Internet access charges, mobile data plans or surcharges, taxes, device repairs and/or replacements.

D) Technical Assistance, DOE O 203.2.4.k, is clarified as follows:

a. Information Technology personnel will provide best effort support for troubleshooting and resolving configuration issues only with the currently approved client virtualized desktop connector application installed on the user's non-GFE device. This is the software application on the non-GFE device that allows it to connect to BPA's myPC environment.

b. Information Technology personnel will not provide onsite or remote troubleshooting or support for a user's non-GFE device related to:

i. Hardware issues

ii. Wired or wireless network configuration or connectivity, except in relation to Guest Wireless Network Access

iii. Internet access or connectivity

iv. Operating system issues

v. Issues related to applications installed locally on the user's non-GFE device (other than currently approved client virtualized desktop connector)

6. Policy Exceptions

There are no exceptions to this policy.

7. Responsibilities

A) The BPA Chief Information Officer (CIO)

a. Sponsors and administers this policy including: overseeing periodic review, ensuring consistency with BPA strategic and operational plans, and meeting regulatory requirements.

b. Reports any significant violations of this policy, or the standards and operations procedures referenced in this policy, to the BPA executive governance body.

B) Information Technology Service Delivery Manager

a. Ensures users of mobile technology are appropriately trained and user agreements are signed prior to providing a GFE mobile device.

C) Authorized System Users

a. Are required to be familiar with current BPA policy regarding the use of mobile 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.

D) BPA Supervisors and Managers

a. Are responsible for ensuring that their organizations are current in their understanding of BPA policy regarding the use of BPA IT services and equipment.

b. 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.

c. Validates the need for the mobile requirement, and provides approval.

E) Information Technology Organization

a. Provides and safeguards the technological architecture that enables mobile device access to BPA IT services and equipment assets, consistent with this policy.

b. Provides current end-user instructions for establishing mobile device connections to BPA IT services and equipment assets.

c. Provides a current list of applications and capabilities available to mobile device users.

d. Configures GFE mobile devices for appropriate access to wireless services.

e. Erases BPA records and data from mobile devices when they constitute a threat to BPA IT services and equipment assets through loss or theft, or when the user ceases to participate in the program.

F) Mobile Technology User

a. Reads and understands this policy, DOE O 203.2, and applicable user agreements to use GFE and/or non-GFE mobile devices consistent with the requirements of these documents.

b. Completes mobile device training as required by the Information Technology organization.

c. Configures non-GFE mobile devices for Guest Wireless Network Access (sponsored guests of BPA).

G) Requisitioners

a. Are responsible for notifying the Contracting Officer (CO) that BPA will furnish IT mobile technology to the contractor.

H) Contracting Officer Representatives (CORs) and Field Inspectors

a. 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.

I) Contracting Officers

a. In the event the contract scope includes BPA furnishing IT mobile technology to contractors, the CO shall ensure the contract includes a requirement for this policy to be observed by contractors.

8. Standards & Procedures

Processes and procedures for requesting and completing IT remote access services are published on the IT Service Desk SharePoint site.

User agreements for the use of mobile technology at BPA are published on the IT Service Desk SharePoint site.

9. Performance & Monitoring

On a continuous basis, a delegate assigned by the CIO shall report any significant violations of this policy:

A) To the CIO.
B) 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 470-8 Business Use of BPA IT Services and Equipment

C) BPA Policy 470-6, Limited Personal Use of BPA IT Services and Equipment

D) DOE O 203.2, Mobile Technology Management

E) HR Directive 410-06-3 Telework and Remote Work Program

F) Title 40 U.S. Code Subtitle III Information Technology Management

11. Review

The policy owner shall review this policy at least every year for relevant purpose, content, currency, effectiveness, and metrics.

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
1.0	5/15/2016	Initial creation by Mike Harris.
2.0	8/18/2016	Per Deputy CIO, modified to remove non-GFE support except for connection to myPC, and restricted guest wireless to sponsored guests of the Agency.
2.1	12/1/2023	Reformatting and grammatical cleanup; synchronize language with current IT policies; expand responsibilities section; add MDM capability.
2.2	12/13/2023	Walked through policy with Paul Dickson and Scott Weaver to update language to a basic standard starting point for wider review. – Mike Harris
2.3	1/25/2034	Reconciled language suggestions from Legal.
2.4	2/10/2024	Reconciled final PWG language suggestions and provided for final review.
2.5	5/15/2024	Received de minimis language suggestions from Labor Relations and reconciled.