

BPA Policy 473-2

Information Technology Systems and Service Policies

Table of Contents

1. Purpose & Background	2
2. Policy Owner	2
3. Applicability	2
4. Terms & Definitions	2
5. Policy.....	4
6. Policy Exceptions	5
7. Responsibilities	5
8. Standards & Procedures	6
9. Performance & Monitoring	7
10. Authorities & References	7
11. Review	7
12. Revision History	7



1. Purpose & Background

The Clinger-Cohen Act of 1996 and the Federal Information Security Management Act of 2002 (FISMA) require the Bonneville Power Administration (BPA) to use a systematic and uniform methodology for providing Information Technology (IT) computing environments. In conjunction with the Federal Information Technology Acquisition Reform Act (FITARA), they create a statutory scheme to clarify the role of the Chief Information Officer (CIO).

The purpose of this policy is to establish requirements related to the technical architecture of BPA's computing environments outlined in the Bonneville Information Technology Architecture (BITA), establish a lifecycle approach to BPA's cyber systems following the System Life Cycle (SLC), and provide requirements for issuing BPA-wide information technology policies to meet requirements outlined in statute.

To supplement these foundational requirements, this policy directs the use of an IT policy library to ensure that the computing environments meet the requirements of BPA's users of IT while remaining in compliance with the laws, rules and regulations that govern BPA's use of IT resources.

This policy directs the use of a technical architecture standard at BPA. The BITA document establishes requirements, authorities and responsibilities related to the technical architecture of BPA's computing environments. The BITA also establishes the list of components available for use in constructing the cyber systems in BPA's computing environments to meet the business requirements for the use of information technology.

This policy directs the use of a documented lifecycle approach to operating and maintaining the collection of components in the computing environments. The BPA SLC defines a multistep process from initiation through disposal of components and cyber systems in BPA's computing environments.

2. Policy Owner

The BPA CIO is the owner of this policy and has the authority to approve written changes to it. The IT organizations are responsible for the implementation and operation of this policy.

3. Applicability

This policy applies to BPA's computing environments including all cyber systems and components, operational technology (OT), and any use of IT at BPA.

4. Terms & Definitions

- A. **Information Technology:** Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange,

Organization Information Technology	Title Information Technology Systems and Services Policies	Unique ID 473-2		
Author M. Harris	Approved by B. Berry, CIO	Date 8/5/2021	Version 2.0	Page 2

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—

1. of that equipment; or
2. 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. (Title 40 USC Section 11101).

- B. Operational Technology (OT):** OT is a subset of IT software, hardware, or service whose function is to directly control or support the operation, maintenance, or monitoring of the electrical grid and that satisfies any of the following:
- 1) accesses or contains memory or storage.
 - 2) has logical access.
- C. IT Equipment:** BPA IT equipment includes but is not limited to BPA’s computer networks and any authorized BPA-owned or -leased computing device or component that can be attached or connected to BPA’s computer network, including any IP-addressable equipment or devices. BPA IT equipment includes desktop computers and monitors, laptop and portable computers, tablets, thin clients and mobile thin clients, firmware, software, shareware, 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 (e.g., flash drives), routers, peripheral devices, multi-purpose machines (e.g., combined facsimile, printer, and copier), and cloud-based IT services such as Archive-as-a-Service, Storage-as-a-Service, Desktop-as-a-Service, Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service, Backup-as-a-Service, etc.
- D. Cloud-based IT Service:** IT service (a sub-component of Information Technology) encompasses several categories of cloud-based services, particularly whenever information is exchanged. Cloud-based services are a software distribution model in which applications are centrally hosted by independent software vendors (ISVs) or application service providers (ASPs) and made available to customers over a network, typically the Internet. Hosted services are a form of cloud-based services in which the vendor runs, manages, and modifies software on behalf of the consumer and manages the consumer data. Software as a Service (SaaS) is another form of cloud-based services in which applications provide the consumer the capability to use the vendor applications

Organization Information Technology	Title Information Technology Systems and Services Policies			Unique ID 473-2
Author M. Harris	Approved by B. Berry, CIO	Date 8/5/2021	Version 2.0	Page 3

running on a cloud infrastructure. The vendor manages all aspects of the application including upgrades.

- E. **Cyber System:** IT equipment or collections of IT equipment; any technology system (or collections thereof) capable of sending, receiving, or storing electronic data. Examples: GridIT, IT, information system, cyber asset, IT system, computing servers, user workstations, remote terminal units, phasor measurement units, network routers and switches.
- F. **Computing Environment:** a structured environment that encompasses software and hardware and provides computer services, support and maintenance. This includes the collection of computer machinery, data storage devices, work stations, software applications and networks that support the processing and exchange of electronic information.

5. Policy

BPA’s IT organizations shall establish, maintain and operate a computing environment for use in official BPA business consistent with laws, rules, and regulations governing its provision and use as established in the following requirements:

- A. **BPA’s Computing Environments:** The CIO or their delegates shall have sole authority to promulgate information technology policies that establish, maintain, and operate BPA’s computing environments.
 - 1. No organizational, functional or programmatic policies, processes, procedures, standards or guidance shall be issued for BPA’s computing environments that conflicts with the policies, guidance, and other governance issued by the CIO or their delegates for BPA’s computing environments.
- B. **BPA’s Technical Architecture:** The CIO shall issue and maintain the technical architecture specifications for BPA’s computing environments.
 - 1. The Office of the CIO (OCIO): Shall document and publish BPA’s IT technical architecture for use by the agency.
 - 2. All cyber systems and enhancements must adhere to the BITA unless granted an exception under the exceptions process defined in the BITA.
- C. **BPA’s IT System Lifecycle:** The CIO shall issue and maintain a documented lifecycle approach for components in BPA’s computing environments.
 - 1. Cyber systems and enhancements or removal of cyber systems must adhere to the SLC for BPA’s computing environments unless granted an exception under the exceptions process defined in the SLC.
- D. **Governance of IT Systems and Services:** The CIO shall issue and maintain supplemental policies, procedures, standards and guidance for the purpose of governance and control

Organization Information Technology		Title Information Technology Systems and Services Policies		Unique ID 473-2
Author M. Harris	Approved by B. Berry, CIO	Date 8/5/2021	Version 2.0	Page 4

of BPA’s computing environments and services not specifically addressed in Section 5.B or 5.C of this policy.

1. **IT Governance Library:** The OCIO shall establish and manage an IT Governance Library to centrally locate all of the CIO’s published supplemental policies, procedures, standards and guidance.
 - a) **Access to IT Governance Library:** Read-only access is provided to all user accounts authorized for BPA network access through the Bonneville User Domain Active Directory. Some documents within the library may be additionally protected if determined by the CIO to be sensitive in nature, and access provided on a need-to-know basis by approval of the CIO.
 - b) **Management of IT Governance Library:** The OCIO manages the content of the IT Governance Library with oversight from the CIO’s management staff and in collaboration with other BPA Information Technology organizations.

6. Policy Exceptions

Exceptions to the BITA may be requested and submitted through the exception process defined in the BITA. The OCIO will adjudicate and document exception requests.

Exceptions to the SLC may be requested and submitted through the exception process defined in the SLC. The OCIO and the IT Program Management Office (IT PMO) will jointly adjudicate and document exception requests and may jointly grant approval for Alternative SLC Work Patterns.

7. Responsibilities

A. The BPA Chief Information Officer (CIO)

1. Sponsors and owns this policy, overseeing periodic review of the policy consistent with BPA strategic and operational plans and all statutory, regulatory and administrative requirements. Reports any critical violations of this policy, or the standards and operations procedures referenced in this policy, to the BPA Executive Governance Body.
2. Serves as the final approval authority for any unresolved differences between the OCIO and the IT PMO in regards to the SLC.

B. The Office of the CIO (OCIO)

1. Is responsible for maintaining BPA’s BITA. This includes reviewing the BITA on a regular basis, and modifying and updating the BITA as required in collaboration with all IT organizations.
2. Is responsible for documenting approval to requests for exception to the BITA.

Organization Information Technology	Title Information Technology Systems and Services Policies			Unique ID 473-2
Author M. Harris	Approved by B. Berry, CIO	Date 8/5/2021	Version 2.0	Page 5

3. Is responsible for resolving any conflicts in the interpretation of the BITA.
4. Is responsible for maintaining BPA’s SLC jointly with the IT PMO. This includes reviewing the SLC on an annual basis, and modifying and updating the SLC as required in collaboration with all IT organizations.
5. Is jointly responsible with the IT PMO for granting approval to alternate SLC work patterns.
6. Is jointly responsible with the IT PMO for resolving any conflicts in the interpretation of the SLC.

C. The IT Project Management Office (PMO)

1. Is responsible for maintaining BPA’s SLC jointly with the OCIO. This includes reviewing the SLC on an annual basis, and modifying and updating the SLC as required in collaboration with all IT organizations.
2. Is jointly responsible with the OCIO for granting approval to alternate SLC work patterns.
3. Is jointly responsible with the OCIO for resolving any conflicts in the interpretation of the SLC.

D. BPA Managers

1. Ensure alignment with policy and engage IT when business needs arise that require an IT system or BPA IT equipment.
2. Coordinate with IT/OT managers and portfolio managers to document their IT automation requirements in the appropriate IT asset category sub-portfolio (Office Automation, Application, Datacenter, Agency Information, Cyber Security, Network Portfolio, etc.).

E. Contracting Officers and Contracting Officer’s Representatives

Ensure that appropriate personnel have certified that IT purchases adhere to BITA standards or have an exception officially documented with the OCIO.

8. Standards & Procedures

Applicable standards for BPA IT equipment are located or referenced within the BITA published by the OCIO and in the IT Governance Library.

Applicable processes, templates and guides for cyber system development and implementation are located or referenced within the SLC published by the IT PMO and in the IT Governance Library.

Organization Information Technology	Title Information Technology Systems and Services Policies			Unique ID 473-2
Author M. Harris	Approved by B. Berry, CIO	Date 8/5/2021	Version 2.0	Page 6

9. Performance & Monitoring

On an annual basis, a delegate of the CIO shall report to the CIO any policies published in the official enterprise-wide policy repository that direct information technology activities and are not published or sponsored through the OCIO. Any exceptions to this policy or critical violations shall be reported to the BPA Executive Governance Body.

10. Authorities & References

- A. Clinger-Cohen Act of 1996, Pub. L. 104-106, 110 Stat. 186 (1996).
- B. Federal Information Security Management Act of 2002 (FISMA), Pub. L. 107-296, 116 Stat. 2259 (2002) (Codified as 6 U.S.C. §§ 511, 512).
- C. Information Technology Management, 40 USC Subt. III §§ 111, 113, 115, 117.
- D. DOE O 200.1A Chg1 (MinChg), Information Technology Management (Jan. 13, 2017).
- E. Federal Information Technology Acquisition Reform Act, H.R. 1232, 113th Congress (2013- 2014) (enacted by Carl Levin and Howard “Buck” McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. 113-291, 128 Stat. 3292 (2014)).

11. Review

This policy shall be reviewed by the policy owner at least every 5 years for relevant purpose, content, currency, effectiveness and metrics.

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
1.0	3/25/2015	Initial creation by Mike Harris from BPAM Chapter 1101 doc.
1.1	5/4/2016	Updates to definitions for consistency across policies, by Mike Harris.
2.0	8/5/2021	Re-written as umbrella policy by Mark Wilczewski and Mike Harris.

Organization Information Technology	Title Information Technology Systems and Services Policies	Unique ID 473-2		
Author M. Harris	Approved by B. Berry, CIO	Date 8/5/2021	Version 2.0	Page 7