BPA Policy 470-2

Removal of User Access to BPA Production Networks and Systems

Table of Contents

1. Purpose & Background

To establish requirements, assign responsibilities, and provide guidance to meet Cyber Security requirements regarding removal of user network and system access when such access is no longer justified or, through routine procedure, when a user's employment has terminated or changed to an inactive status.

User access to networks and systems that remain when changes occur in the employment status, job function, or duties of employees contributes to increased risks to the BPA computing environment and risk of regulatory non-compliance, financial fraud, and/or unauthorized disclosure of various categories of information requiring protection.

2. Policy Owner

The BPA Chief Information Officer (CIO) is the owner of this policy.

3. Applicability

All organizations and staff within BPA, regardless of geographical location or purpose, are required to adhere to this policy.

This policy does not address non-routine changes to a user's employment status, including releases, terminations or other BPA-initiated actions.

The provisioning of user accounts, shared accounts, special accounts, password control, etc. is addressed under separate policy.

Other than notification requirements, this policy does not establish operational or administrative procedures for effecting its implementation.

4. Terms & Definitions

A. **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.

B. **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.

C. **IT Service**, (a sub-component of Information Technology) encompasses several main categories such as managed staffing, managed services, consultant arrangements, and cloud-based services, particularly whenever information is exchanged. In order to distinguish cloud-based services from data subscription, cloud-based services is 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 client and manages the clients' data. Software as a Service (SaaS) is another form of cloud-based services in which applications provide the consumer the capability to use the provider's applications running on a cloud infrastructure. The provider manages all aspects of the application, including upgrades.

D. **Cyber System**: IT equipment or collections of IT equipment; any technology system (or collections thereof) capable of sending, receiving, or storing electronic data. Synonyms: GridIT, IT, information system, cyber asset, IT system. Examples: computing servers, user workstations, remote terminal units, phasor measurement units, network routers and switches, etc.

5. **Policy**

Upon a routine material change in an employee's employment status (e.g. retirement, resignation etc.), an employee's manager or Contracting Officer's Technical Representative (COTR) or Field Inspector must communicate the change to the HR Help support group. The HR Help support group shall generate a daily Notification Report and distribute that report to all relevant parties, including the Hardware Operations Server Access Control Group (SAC). The SAC is required to subsequently and in a timely manner not to exceed one business day communicate the change to the Server Operations manager, Software Operations Application Security Administration Group (ASA), and the Control Center

Privileges Group. Within the same day of notification, each of these groups is required to ensure that access is removed from the networks and systems to which the employee has authorized access.

Material changes in the permissions needed to support an employee's job duties (e.g. Root or Administrator level privilege, etc), should be communicated directly to the appropriate System Security Manager of the network or system to which the employee already has authorized access.

The employee's manager or COTR or Field Inspector must ensure that communications are accurate and performed immediately upon initiation or discovery of the changes to the employee's employment status or job functions.

6. **Policy Exceptions**

There are no exceptions to this policy.

7. **Responsibilities**

A. **BPA Chief Information Officer (CIO)**

Sponsors and owns this policy, overseeing periodic review of the policy, consistent with BPA strategic and operational plans and all statutory, regulatory, administrative, and OMB requirements. Reports any critical violations of this policy, or the standards and operations procedures referenced in this policy, to the BPA Executive Governance Body.

B. **BPA Mangers, COTRs, and Field Inspectors**

Report to HR Help in a timely manner as described above any routine material change in an employee's employment status.

C. **SAC**

Remove access to networks and systems in a timely manner for users identified within the HR Help Notification Report.

8. **Standards & Procedures**

Applicable standards for user access to BPA IT Equipment, IT Services, and Cyber Systems are located or referenced within the Bonneville Information Technology Architecture (BITA) published on the Chief Technical Officer (CTO) SharePoint site.

9. **Performance & Monitoring**

On a regular basis SAC shall report to the Hardware Operations Manager any user access status that differs from that indicated by Human Resources.

10. **Authorities & References**

A. DOE O 200.1A, Information Technology Management

B. Clinger-Cohen Act of 1996

C. BPA Policy 473-2 Information Technology Policies

D. 40 U.S. Code SUBTITLE III: INFORMATION TECHNOLOGY MANAGEMENT

11. **Review**

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

12. **Revision History**

Version	Issue Date	Description of Change
1.0	3/25/2015	Initial creation by Mike Harris from Cyber Security CSO-20070529-01 doc.
1.1	5/4/2016	Updates to definitions for consistency across policies, by Mike Harris.