

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE
INFORMATION TECHNOLOGY STANDARD

Name Of Standard: Windows Server Security	Number: STD-SES001
Domain: Platform	Category: Network Platform
Date Issued: 04/02/2002	Issued By Direction Of:
Date Reviewed: 02/10/2011	 James Weaver, Dir of Div of Tech Engineering

Abstract:

The Department of Public Welfare (DPW) distributed environment is comprised primarily of servers running Windows Server Operating Systems. The growth of this environment and the resulting increase of hosting of confidential data in this environment require definition, adoption, and enforcement of appropriate security standards to ensure the protection of that data.

General:

The purpose of this document is to define the security standards for protecting Windows server resources and data at DPW.

Standard:

Windows Server Security

The Division of Technology Engineering (DTE), Systems Engineering Section (SES), Enterprise Operating Systems Unit (EOSU) designs and maintains security within DPW's distributed Windows networking environment. EOSU researches, evaluates, tests, and deploys security solutions for that environment, and recommends, drafts, and maintains related security standards.

The Need for Security Standards

Windows server security standards are necessary to ensure that hardware and operating systems are "hardened," or secured, to minimize the threat of hacking and sabotage, that could result in service interruption or the theft or destruction of data.

Scope of Standards

The standards apply to servers running Windows Server Operating Systems, VMware on DPW's production network. They also apply to BackOffice and other server-hosted applications and resources, as well as the architectural design of the Windows logical networking environment.

The Standards

In addition to existing [Governors Office of Administration \(GOA\) Office of Information Technology \(OIT\) standards](#), DPW has adopted [National Security Agency \(NSA\) standards](#) and Microsoft Corporation recommended practices as the minimum standards for securing the Windows network, servers, and server-hosted applications and resources. Security configuration on all DPW servers must adhere to these standards.

Secure Implementation of Standards

EOSU ensures these standards are implemented on DPW servers managed by the Bureau of Information Systems (BIS), and provides security configuration information to designated program office personnel for implementation on servers under their control.

Such information, whether in the form of security templates or configuration guidelines, are confidential and must be stored under lock and key, and accessed on a need-to-know-basis.

Hotfixes and Patches

EOSU subscribes to reviews-related security bulletins and notifications from the [CERT\(r\) Coordination Center](#), Microsoft, and other recognized Windows-related server and networking security authorities to maintain an awareness of current security threats and security-related hotfixes and patches.

EOSU determines the need to apply hotfixes and patches. They analyze and review the technical merit of each fix or patch as it relates to agency server configurations and the Windows networking environment. EOSU then recommends to the BIS Security Officer whether or not a particular fix or patch should be deployed within the DPW server environment, and if so, on which servers. If approved, the Security Officer will notify Program Office Security Monitors. Any recommendation for non-deployment will include a brief justification.

EOSU also provides technical support related to the application of security patches.

Secure Distribution of Files

EOSU ensures that files are distributed to Security Monitors or designated points of contact for server security maintenance. EOSU designs a distribution process for this purpose. Contact EOSU for more information.

Server Security Audits

EOSU develops the process for conducting server-security audits and conducts the audits in collaboration with the BIS Security Officer. The objective of these audits is to identify risks and overall compliance with existing server security standards.

Future Auditing and Application of Hotfixes and Patches

EOSU continues to research and deploy solutions that extend the capability to automate and reduce the administrative overhead related to security monitoring, reporting, administration, and maintenance within the Windows networking environment.

Exemptions from this Standard:

There will be no exemptions to this standard.

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DPW Information Technology Standards Team.

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
04/02/2002	1.0	Initial Creation	Bob Minck
04/08/2002	1.1	Edited for style.	Beverly Shultz
06/11/2004	1.2	Deleted Netlq section	John Foy
06/17/2008	2.0	Changed language	John Foy
02/10/2011	2.1	Reviewed content – No changes	John Foy