

***ITS Security Procedure: Trusted Area File Server
UNMC Information Technology Services***

INTRODUCTION

The purpose of this policy is to ensure that appropriate steps are taken to secure UNMC file servers and other client server systems. This policy applies to all UNMC and business partner file servers and systems that are connected to the UNMC network infrastructure.

BASIS FOR POLICY

UNMC strives to maintain an environment of quality patient care, research, and education. In order to maintain this environment, steps must be taken to ensure that access to important information on computing systems is not compromised, interrupted, or derogated. File servers and client server systems not only help enforce network security policies but are also the typical point of attack and therefore special security measures are needed to ensure quality.

DEFINITIONS

File Server A File Server is any system that provides or shares resources (files, drives, printing, applications, etc.) with any other system. For the basis of this policy, the term "file server" will also encompass other client server based information systems such as the HP NonStop Server, Active Directory Servers and etc.

DMZ A DMZ or Demilitarized Zone is a network that is separated from an organization's internal protected network and logically sits between the organization and the unsecured public Internet. A DMZ usually has special security measures implemented and is used to provide the public presence of an organization's information technology.

Trusted Network For this policy, "trusted network" is defined to be all UNMC/NHS/UMA owned or managed internal data communication networks without incoming direct public access.

Mission Critical System Any system that is necessary to conduct the day-to-day business operations of UNMC.

Remote Access: Non hard wired console access to a file server.

POLICY

A. Location

It is highly recommended that all file servers be physically located in UNMC ITS managed data centers. If a mission critical system is not located in one of the approved data centers, the unit management must ensure that the server is physically secure.

B. Hardening the Operating System and Applications

All file servers must be "hardened". Hardening is the process of shutting off unnecessary protocols and services and applying necessary security patches to the operating system and applications on the system. Where feasible, file servers will be scanned for vulnerabilities before allowing access to the UNMC trusted network. File servers will also be scanned and audited, periodically, for new vulnerabilities. Should a vulnerability or security risk that threatens the trusted network be found, UNMC ITS may temporarily disconnect a file server from the trusted network until it has been determined that the vulnerability has been patched or the security risks have been mitigated. System administrators should ensure that no "back doors" access the server.

C. Passwords

All file servers must comply with UNMC password policies. (See UNMC ITS Security Procedure: Passwords) Steps must be taken to ensure that passwords are not sent over the trusted network in "clear text." For servers that are located in an UNMC ITS managed data center, an account should be established for use by the operations staff. This account would be utilized for verification that the system is operational when resolving problems.

D. Content

The content on all systems connected to the UNMC private network must comply with UNMC policies. Where technically feasible, systems that contain patient identifiable information require personal authentication. It is also recommended that encryption of selected data fields be used where appropriate.

E. Communication

Communication to or from trusted area file servers will be limited to the internal trusted network and to the DMZ on a restricted basis. (See UNMC ITS Security Procedure: DMZ and Network Access Control policies) No direct access from the public Internet will be allowed to any file server on the internal trusted network. Systems requiring public access will need to be placed in the DMZ or will need to be accessed indirectly through a hardened system in the DMZ. Out-

going Internet access should be restricted where possible (See UNMC ITS Security Procedure: DMZ and Network Access Control policies)

F. Protocols

The preferred communication protocol on the UNMC/NHS/UMA trusted network is currently TCP/IP. The use of other network communication protocols must be coordinated with ITS.

G. Disaster Recovery

A 24x7x365 contact will be provided to UNMC Operations for any system placed in the UNMC managed data center. Systems in the trusted area must comply with UNMC Business Continuity Plan (See UNMC ITS Security Procedure: Business Continuity Plan)

H. Authentication

All file servers must have authentication.

I. Remote Administration

It is recommended that when utilizing remote administration of a server strong authentication should be implemented.

J. Banners

Where possible, all servers should display a login banner, that says, "If you are not an authorized user of this system, disconnect immediately".

K. Auditing

Where possible, system administrators must enable logging and auditing functions on systems they administer. Operating system audit logs should be reviewed periodically. Any suspicious activity found in audit logs should be brought to the attention of the ITS Helpdesk as soon as possible. (See UNMC ITS Security Procedure Incident Response Procedure)