

DMZ Policy and Guidelines

INTRODUCTION

The purpose of this policy is to ensure that appropriate steps are taken to secure UNMC systems with public Internet presence. This policy applies to all UNMC and business partner systems placed in the DMZ or with direct or indirect access to or from the Internet.

DEFINITIONS

Internet The Internet is the collection of interconnected networks that are external to UNMC/NHS/UMA networks.

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.

Extended DMZ is the part of the DMZ which does NOT reside in the UNMC ITS managed data centers.

POLICY

A. Location

Systems requiring public access should be placed inside the UNMC ITS managed data centers. Providing there is a valid business or academic need, the DMZ network can be extended beyond the UNMC ITS managed data centers to selected locations. When a server is installed in an extended DMZ, the system administrator and ITS will jointly work to ensure that the server is technically secure. The system administrator must ensure that the servers are physically secure.

B. Hardening the Operating System and Applications

All systems to be placed in the DMZ 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. Systems to be placed in the DMZ will be scanned for vulnerabilities before allowing access from the public Internet and all systems in the DMZ will be scanned and audited periodically for new vulnerabilities by UNMC ITS. Scanning will be done in such a manner that the systems will not be interrupted. If a scan has the potential for disrupting systems, the system administrator will be involved in scheduling the scan. Should a vulnerability or security risk that threatens the network be found, UNMC ITS may temporarily disconnect a file server from the 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” or modems access the server.

The following services should be avoided:

anonymous ftp	finger
P2P (Peer to Peer)	smtp (only allowed to approved mail gateways)
ICQ and IRC	nfs
snmp	small services (echo, discard, chargen, etc.)
rpc	

C. Passwords

All systems to be placed in the DMZ where technically feasible must comply with UNMC password policies. Steps must be taken to ensure that passwords are not sent over the Internet in “clear text”. Whenever possible, passwords should not be stored locally on the systems with public access and a means of external authentication is preferred. 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 placed in the DMZ must comply with UNMC policies. The content on all systems in the DMZ should be for business or academic use only. All systems to be placed in the DMZ should not store any patient identifiable or proprietary information on the local system. DMZ systems that are used to access patient identifiable information should incorporate strong authentication and should retrieve patient identifiable information from a secured system only when needed. (See FTP Policy.)

E. Communication

Systems placed in the DMZ will communicate in the following manner:

- | | |
|-----------------------------|---|
| 1. Other systems in the DMZ | No restrictions |
| 2. Internet | Port to port basis as implemented by firewall |
| 3. Trusted area | Port to port basis as implemented by firewall |

F. Protocols

The system administrators for any systems to be placed in the DMZ will provide the UNMC Network Team with documentation of all communication protocols, ports, and direction of network traffic so that appropriate firewall rules can be implemented. (See Network Access Control Policy.)

G. Disaster Recovery

A 24x7x365 contact will be provided to UNMC Operations for any system placed in the DMZ. All systems to be placed in the DMZ which require a backup, need to ensure that the backup does not traverse the firewall. Systems in the DMZ must comply with UNMC Business Continuity Policy ([link to Business Continuity Policy](#))

H. Periodic reviews

ITS Network Team and the system administrators will periodically review the systems in the DMZ to ensure that appropriate technology is being employed to adequately secure the server. These reviews will include a physical visit to Extended DMZ sites.

I. DMZ Adds or Changes

When a system administrator who does not currently have a file server in the DMZ requests that a new file server be added to the DMZ, the UNMC ITS Security Officer will coordinate a meeting with the system administrator and ITS Network Team to review the DMZ architecture.

DMZ changes need to occur in a timely manner to ensure that access is uninterrupted. All DMZ requests should be e-mailed to dnsadmin@unmc.edu. All requests will be processed within 7 working days from date of request. If this is an emergency, please indicate this in the email, and your request will be expedited. An email will be sent to the requestor when the request has been completed.