Information Services & Technology
DMZ Equipment Deployment Process

I. PURPOSE

This document describes the policy under which organizations deploy equipment into DMZ networks for the purpose of transacting business related to UMDNJ. This policy is designed to minimize the potential exposure to UMDNJ from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of UMDNJ resources.

Devices that are Internet facing are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside on a less secure network.

II. APPLICABILITY

All equipment or devices deployed in a DMZ owned and/or operated by UMDNJ (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by UMDNJ, must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "UMDNJ.edu" domain or appears to be owned by UMDNJ.

All new equipment which falls under the scope of this policy, must be configured according to the referenced configuration documents, unless a waiver is obtained from IS&T. All existing and future equipment deployed on UMDNJ's un-trusted networks must comply with this policy.

III. ACCOUNTABILITY

Under the President, the Senior Vice Presidents shall ensure compliance with this policy. The Vice President for Information Systems and Technology (IST), the President/CEOs of the Healthcare Units, Deans and Vice Presidents shall implement this policy by means of system specific procedures, guidelines and standards.

IV. DEFINITIONS

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sponsoring Organization</td>
<td>The UMDNJ organization who requested DMZ access to UMDNJ.</td>
</tr>
</tbody>
</table>

V. POLICY

A. Pre-Requisites

1. Security Review

All new DMZ connectivity will go through a security review with the Information Security department (IS&T). The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.
2. **Business Case**
All production DMZ connections must be accompanied by a valid business justification, in writing, that is approved by a Manager or Director. Typically this function is handled as part of the **DMZ Equipment Deployment Agreement**.

3. **Point of Contact**
The Sponsoring Organization shall designate a person to be the Point of Contact (POC) for the DMZ connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the **DMZ Equipment Deployment Agreement** that pertain to it. In the event that the POC changes, the relevant IS&T department must be informed promptly.

B. **Establishing a Connection**
Sponsoring Organizations within UMDNJ that wish to establish connectivity in the DMZ are to file a DMZ Equipment Deployment request with the IS&T Service Center. The IS&T Service Center will engage the IS&T Security Team to address security issues inherent in the project. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to IS&T, as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review.

C. **Modifying or Changing Connectivity and Access**
All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via the IS&T change management process. The Sponsoring Organization is responsible for notifying IS&T when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

D. **Terminating Access**
When access is no longer required the Sponsoring Organization within UMDNJ must notify IS&T. IS&T will then terminate the access. IS&T Security teams must conduct an audit of DMZ system access on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be deprecated, and/or are no longer being used to conduct UMDNJ business, will be terminated immediately. Should a security incident or a finding that a connection has been deprecated and is no longer being used to conduct UMDNJ business necessitates a modification of existing permissions, or termination of connectivity IS&T will notify the POC or the Sponsoring Organization of the change prior to taking any action.

VI. **NON-COMPLIANCE AND SANCTIONS**
Any person found to have violated this policy may be subject to denial or removal of access privileges to the University network; disciplinary action under applicable University policies and procedures up to and including termination; civil litigation; and/or civil or criminal prosecution under applicable state and federal statutes.