NORTHERN
NEW MEXICO COLLEGE

Your school, your future.

Firewall Policy

Purpose

NNMC operates perimeter firewalls between the Internet and its private internal network in order to create a secure operating environment for [company name]'s computer and network resources. A firewall is just one element of a layered approach to network security. The purpose of this Firewall Policy is to describe how NNMC firewall will filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access for business users.

The Firewall Policy is subordinate to NNMC's general Security Policy, as well as any governing laws or regulations.

Scope

This Firewall Policy refers specifically to the [name firewall] firewall. The role of this firewall is to protect internal systems and restrict unwanted access into the Network. The firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks.
- Block unwanted traffic as determined by the firewall rule set.
- Hide vulnerable internal systems from the Internet.
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet.
- Log traffic to and from the internal network.
- Provide robust authentication.
- Provide virtual private network (VPN) connectivity.

All employees of NNMC are subject to this policy and required to abide by it.

Responsibilities

NNMC IT department is responsible for implementing and maintaining firewalls, as well as for enforcing and updating this policy. Logon access to the firewall will be restricted to a primary firewall administrator and one designee. Password construction for the firewall will be consistent with the strong password creation practices outlined in NNMC's Password Policy.

Any questions or concerns regarding NNMC firewall should be directed to Jorge C. Lucero ext. 258.

Policy

The approach adopted to define firewall rule sets is that all services will be denied by the firewall unless expressly permitted in this policy. The NNMC firewall permits the following outbound and inbound Internet traffic.

- Outbound – All Internet traffic to hosts and services outside of NNMC.
- Inbound – Only Internet traffic from outside that supports the business mission of NNMC as defined by our Mission Statement. Ex. Servers only.

The table below identifies the most common services used for Internet communications within the NNMC's environment. For each service type, the table will indicate whether the firewall will accept it, accept it with authentication, or reject it.

Traffic/Service	**Port**	**Outbound (internal to external)**	**Inbound (external to internal)**	**Inbound VPN (secure VPN to internal)**	**Comments**
DNS					
Finger					
FTP					
gopher					
HTTP					
ICMP					
IMAP					
LDAP					
NFS					
NNTP					
NTTP					
POP3					
TFTP					

Telnet					
NFS					
NetBIOS					
RPC					
Rsh					
SMTP					
SNMP					
SSH					
X Windows					
[Insert service]					
[Insert service]					

Operational Procedures

- NNMC employees may request changes to the firewall's configuration in order to allow previously disallowed traffic. A firewall change request form, with full justification, must be submitted to the IT department for approval. All requests will be assessed to determine if they fall within the parameters of acceptable risk. Approval is not guaranteed as associated risks may be deemed too high. If this is the case, an explanation will be provided to the original requestor and alternative solutions will be explored.

- NNMC employees may request access from the Internet for services located on the internal [company name] network. Typically, this remote access is handled via a secure, encrypted virtual private network (VPN) connection.

  VPN sessions will have an absolute timeout length of 1 day. An inactivity timeout will be set for 1 day. At the end of these timeout periods, users must re-authenticate to continue or re-establish their VPN connection. A VPN connectivity request form, with full justification, must be submitted to the IT department for approval. Approval is not guaranteed.

- From time to time, outside vendors, contractors, or other entities may require secure, short-term, remote access to [company name]'s internal network. If such a need arises, a third-party access request form, with full justification, must be submitted to the IT department for approval. Approval is not guaranteed.

- Turnaround time for the above stated firewall reconfiguration and network access requests is approximately 6 days from the receipt of the request form.

- Firewall logs will be backed up, reviewed and archived.

Enforcement

Wherever possible, technological tools will be used to enforce this policy and mitigate security risks. Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Agreement

I have read and understand the Firewall Policy. I understand if I violate the rules explained herein, I may face legal or disciplinary action according to applicable law or company policy.

Name: ____

Signature: ____

Date: ____