IT Security
Agency Policies and Procedures

Firewall Change Control Procedure

Policy Objectives:
The purpose of this document is to define Admin's process for Requesting Firewall Rule Changes and Firewall Rule Reviews.

Background Information:
Department of Administration's (Admin) Firewall Change Control Procedure outlines the roles, responsibilities and procedures for compliance with the Minnesota State Office of Enterprise Technology Firewall Rule Change Process.

Scope:
This procedure is applicable to all Department of Administration employees, and contractors that are required to work with firewalls or to request rules to enable new IT services. Failure to comply with this policy could result in disciplinary action, up to and including termination of employment.

Responsibilities:

Employees must:

- Follow Firewall Change Control procedures as described herein.
- Report violations of standards to the Chief Information Officer and their direct supervisor.

Managers must:

- Familiarize themselves with all IT Security Policies.
- Read, understand, and support the IT Security Policies that pertain to their groups function.
- Ensure employees read all applicable IT Security Policies, Standards and procedures required to perform their duties.
- Understand who has a legal or statutory requirement to access information under their control.

Chief Information Officer must:

- Implement only approved firewall rules which are in line with the Office of Enterprise Technology's (OET) firewall default security policy.
- Evaluate risk and recommend mitigation for rules that do not meet the default policy but have a business need .
- Monitor firewall rules and provide reports to the Department of Admin for rule review and exception management.

Requirements:

General

- **Firewall Rule Requests**
  - Maintain a list of approved Firewall Change Requestors and send to OET. Update annually or when personnel changes occur.
  - Firewall rule changes must be documented with a business service need for the change.
  - Firewall rule changes must be made in accordance with the OET firewall default security policy. If not, a business justification must be forwarded with the request to document why an exception to the default policy should be considered.
  - The Department of Administration firewall rule requests must be created by authorized Firewall Change Requestors.
  - Firewall rule change requests must document a required implementation date and time that firewall services are required.
  - Firewall rule changes must be submitted to OET change management in accordance with the published OET Firewall Rule Change Process. Lead times for OET to accomplish changes must be account for as listed in the OET Change Control process.
  - The justification or business need for the firewall rule will be entered into the firewall rule comment field for documentation purposes.

- **Approval**
  - Firewall changes must be approved by Firewall Change Requestor and reviewed by the Chief Information Officer or his/her delegate prior to submitting a firewall change request.
  - Maintain a record of all firewall change approvals.

- **Testing of Changed Firewall Rules**
  - The change requestor will ensure that the change will be tested once the change to the firewall is implemented.
  - The change requestor is accountable to ensure that the change requested was performed.

- **Firewall Rule Reviews and Recertification**
  - IP addresses that identify Department of Administration IT devices shall be documented. Network maps shall also be maintained to identify all Department of Administration network segments used in firewall rule requests.
  - At least annually, Admin must ensure that OET provides a report of all firewall rules that relate to the Department of Administration's IP addresses as documented in the OET/Admin SLA in appendix A.
  - At least annually, Admin must review all rules that affect its services and recertify the business need.
  - Any rules that cannot be validated should be suspended until a business need can be determined. If, upon suspension, the business is identified at a later time, the rule can be turned back on. Delete rules after 30 days of suspension and no business need is identified.
  - The completed rule review shall be signed by the business owner or delegated authority. There will be multiple division reviews required to assemble the entire rule review but all segment rule reviews will be forwarded to the CIO/CISO for review and final approval.

- **Firewall Administration and Maintenance**
  - OET will provide all administration and maintenance of firewall platforms in accordance with OET/ADMIN Service Level Agreements or inter agency agreements.

Glossary:

Firewall Rule
A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass.

Appendix A
OET/ADMIN SLA

Enterprise Firewall Services Task Matrix

Description

Firewall Services provides infrastructure design, configuration, rule sets, management and monitoring. The service is available to customers of OET WAN services.

OET provides comprehensive firewall services including management, monitoring and incident management. The service can include acquisition of premise-based firewall hardware, or network based firewall instances. Alternatively, customers can provide current Cisco firewall hardware for OET to manage. Firewalls are managed per the *Firewall Change Implementation* Process.

**Customers using OET WAN services for connection to MNET can add firewall services to these connections. This can be a centralized firewall with a statewide MPLS VPN behind it, or premise based firewall between the WAN and LAN.

Features & Benefits:

- Circuit-level gateways
- Application-level gateways
- OET Service Desk 24/7 technical support
- Designed service, tailored to the individual requirements of the customer using standard OET rates.

OET & Customer Responsibilities:

Enterprise Firewall Services	Daily	Weekly	Monthly	Quarterly	Semi-Annually	Annually	One Time	As Needed	Comments
OET Firewall Responsibilities									
Firewall Administration									
1. Backup configuration	X								
2. Maintain hardware								X	
3. Maintain/patch software								X	
4. Implement rule set changes per: *Firewall Rule Change Process*								X	
5. Implement Emergency rule set changes per *OET Change Management Policy*								X	
6. Provide customer with current rule set						X			
7. Validate s/w and h/w versions are				X					

Enterprise Firewall Services	Daily	Weekly	Monthly	Quarterly	Semi-Annually	Annually	One Time	As Needed	Comments
currently supported									
Reporting and Logging									
1. Backup and retain traffic logs for 90 days	X								
2. Backup and retain administrator logs for 13 months	X								
3. Monitor systems for uptime and security events	X								
Incident Management									
1. OET will notify customer of unplanned outages per OET *Service Level Objectives For Resolution*								X	
Security Incident Management									
1. OET will notify customer of critical security incidents within 1 hour								X	
Business Continuity									
1. OET will recover system based upon recovery time objectives								X	
2. OET will support customer's business continuity testing						X			
Customer Firewall Responsibilities									
Firewall Administration									
1. Assume responsibility for firewall rule set								X	
2. Document business rationale for each rule								X	
3. Recertify rule set annually						X			Quarterly in 2013
4. Maintain/validate list of authorized staff to request changes						X			
5. Maintain current network diagram, supply to OET as requested								X	Joint responsibility until network separation
Reporting and Logging									
1. Review each report and document action of critical issues								X	
2. Inform OET of detailed logging requirements									After network separation
Incident Management									
1. Provide 7X24 contact list for critical incidents								X	Business contact

Enterprise Firewall Services	Daily	Weekly	Monthly	Quarterly	Semi-Annually	Annually	One Time	As Needed	Comments
2. Respond to Critical incidents within 1 hour and confirm resolution								X	
Security Incident Management									
1. Provide 7X24 contact list for security incidents								X	Business contact
2. Respond to Critical security incident within 1 hour								X	
Business Continuity									
1. Support annual business continuity test						X			
2. Support disaster declaration								X	
3. Notify OET 90 days prior to customer test								X	

Notes/clarification/assumptions:

1. Firewall is connected to Admin facilities