BERGRIVIER MUNICIPALITY

FIREWALL POLICY

APRIL 2012

Firewall Policy

A firewall is an appliance (a combination of hardware and software) or an application (software) designed to control the flow of Internet Protocol (IP) traffic to or from a network or electronic equipment. Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Rule set. Firewalls represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include, but are not limited to, antivirus software, intrusion detection software, patch management, strong passwords/passphrases, and spyware detection utilities.

Firewalls are typically categorized as either “Network” or “Host”: a Network Firewall is most often an appliance attached to a network for the purpose of controlling access to single or multiple hosts, or subnets; a Host Firewall is most often an application that addresses an individual host (e.g., personal computer) separately. Both types of firewalls (Network and Host) can be and often are used jointly.

This policy statement is designed to:

- A Network Firewall is required in all instances where Sensitive Data is stored or processed;
- Raise awareness on the importance of a properly configured (installed and maintained) firewall.

Definition:

Term	Definition
Electronic Equipment:	All Bergrivier Municipality owned or issued related equipment (e.g. servers, workstations, laptops, PDAs, printers, fax and other such devices) that attaches to the municipal network, or is used to capture, process or store municipal data, or is used in the conduct of municipal business.
Firewall:	Any hardware and/or software designed to examine network traffic using policy statements (rule set) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.
Firewall Administrator:	The Municipality’s function charged with the responsibility of Firewall Configuration and/or Rule set administration. Administrative duties typically include implementation and documentation of approved changes, analysis of activity logs, and execution and documentation of reviews of system settings and/or rule sets.
Firewall Configuration:	The system settings affecting the operation of a firewall appliance.
Firewall Rule set:	A set of policy statements or instructions used by a firewall to filter network traffic.
Host:	Any computer connected to a network.
Internal Information:	Information that is intended for use by and made available to members of the municipal community who have a business need to know.

Legally/Contractually Restricted Information:	Information that is required to be protected by applicable law or statute.
Network Device:	Any physical equipment attached to the municipal network designed to view, cause or facilitate the flow of traffic within a network. Examples include, but are not limited to: routers, switches, hubs, wireless access points.
Network Extension:	Any physical equipment attached to the municipal network designed to increase the port capacity (number of available ports) at the point of attachment. Examples include, but are not limited to: routers (wired and wireless), switches, hubs, gateways.
Network Firewall:	A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).
Public Information:	Information that is available to all members of the municipal community, and may be released to the general public. The Municipality reserves the right to control the content and format of Public Information. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Examples include the Municipality's auditable financials.
Sensitive Data:	See “Legally/Contractually Restricted Information” above.
Municipal Network:	The network infrastructure and associated devices provided or served by the Municipality.

Policy Statement:

Where Electronic Equipment is used to capture, process or store data identified as Municipal “Legally/Contractually Restricted” and the Electronic Equipment is accessible via a direct or indirect Internet connection, a Network Firewall appropriately installed, configured and maintained is **required**.

All installations and implementations of and modifications to a Network Firewall and its Configuration and Rule set are the responsibility of the IT Department.

Where Electronic Equipment is used to capture, process or store data identified as Municipal “Internal” or “Public” and the Electronic Equipment is accessible via an Internet connection, a Host and/or Network Firewall is **recommended**.

Procedures:

a. The Request for Firewall Rule set Modification Form is used to:

   1. Request and document all changes to Network Firewall Rule sets where Firewall Administration is performed by the IT Department. All requests are subject to the approval of the IT Department and review by the Director or it’s designate.

b. All related documentation is to be retained by the Firewall Administrator for three years and is subject to review by Internal Audit.

1. All Firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default (the initial Rule set should be set to “logging or learning mode” to prevent service interruptions). The Rule set should be opened incrementally to only allow permissible traffic.

2. Firewalls must be installed within production environments where “Legally/Contractually Restricted Information” is captured, processed or stored, to help achieve functional separation between web-servers, application servers and database servers.

3. Firewall Rule sets and Configurations require periodic review to ensure they afford the required levels of protection:

   a. The IT Department must review all Network Firewall Rule sets and Configurations during the initial implementation process.

   b. Firewalls protecting municipal Systems must be reviewed semi-annually;

   c. The IT Department must retain the results of Firewall reviews and supporting documentation for a period of three (3) years; all results and documentation are subject to review by the IT Department and Internal Audit.

4. Firewall Rule sets and Configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required. Access to rule sets and configurations and backup media must be restricted to those responsible for administration and review.

5. Network Firewall administration logs (showing administrative activities) and event logs (showing traffic activity) are to be written to alternate storage (not on the same device) and reviewed at least weekly, with logs retained for 90 days. It is recommended that utilities or programs that facilitate the review process be employed. Appropriate access to logs and copies is permitted to those responsible for Firewall and/or system maintenance, support and review.

6. The IT Department will execute approved changes to the Firewall Rule sets maintained <u>scheduled maintenance window</u>.

7. The IT Department will perform changes to Firewall Configurations according to approved production maintenance schedules.