WILLIAMSBURGH
HOUSING ASSOCIATION

Firewall Policy and Procedure

Revision History

Revision Date	Reviewer(s)	Review Date	Description of Revision
March 2022	Finance and IT	March 2023	New Policy

This policy can be made available in different languages and other formats such as Braille, large print or tape, on request.

Contents

1.Summary

Williamsburgh Housing Association (WHA) will implement a firewall between the Internet and private internal network in order to create a secure operating environment for the Associations 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 the firewall will filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access.

This policy refers specifically to the WatchGuard M370 firewall already installed in WHA's premises. 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.
- 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.

This policy is applicable to all WHA 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.

2.Requirements

2.1 All installations and implementations of and modifications to a Firewall and its Configuration and Rules are the responsibility of the IT Officer and IT Assistant with this exception: maintenance of a Firewall Rule may be performed by our external IT Support Company.

2.2 Access to the Firewall is governed by password authentication. Only the IT Officer, IT Assistant and IT Support Company are permitted access to the Firewall. Any changes to the device must be performed by either of the IT Officer, IT Assistant and IT Support Company roles. No other member of staff is authorised or capable of accessing the Firewall.

2.4 The Firewall physical device is housed in a secure area of WHA's premises. This location is restricted through the use of secure key and may only be accessed by a restricted number of authorised members of staff.

2.5 The Firewall will provide access to the network only through a restricted number of ports. Any port that is not used to provide a connection will be disabled to prevent unauthorised access and ensure the network security is maintained.

2.6 There is a requirement for equipment to be used out with WHA therefore Windows Firewall (Software) will be in use at all times.

2.7 All Firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default. The Rules should be opened incrementally to only allow permissible traffic.

2.8 Firewall Rules and Configurations require periodic review to ensure they afford the required levels of protection:

2.9 IT Officer must review all Network Firewall Rules and Configurations during the initial implementation process.

2.10 Firewall Rules and Configurations must be backed up frequently to alternate storage media in order to preserve the integrity of the data, should restoration be required. Access to rules and configurations and backup media must be restricted to those responsible for administration and review.

2.11 Network Firewall administration event logs (showing traffic activity) are to be reviewed from time to time. Appropriate access to logs and copies is permitted to those responsible for Firewall and/or system maintenance, support, and review.

3. Operational Procedures

3.1 Additions or changes to the firewall's configuration may be requested to allow previously disallowed traffic. A change request form, with full justification, must be submitted to the IT Officer for approval. This will be reviewed by the Finance and IT Manager and IT Officer and approval granted or rejected.

3.2 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 high. If this is the case, an explanation will be provided to the original requestor and alternative solutions will be explored.

3.3 Employees working from home may require access to internal services. Typically, this remote access is handled via a secure, encrypted virtual private network (VPN) connection.

3.4 From time to time, external service providers, contractors, or other entities may require secure, short-term, remote access to the Association internal network. Should such a need arise, an access request form, with full justification, must be submitted to the IT Officer for approval. Approval is not guaranteed.

3.5 The IT Officer will ensure that the change will be tested once the change to the firewall is implemented.

3.6 The change requestor is responsible to ensure that the change requested was performed and functions as per their requirements.

3.7 There is a need to allow Read Only access to our firewall to troubleshoot any issues by Watchguard Support. This is restricted by their External IP address. IT Officer or IT Assistant must also enable Support Access on the Firewall and provide support with a one time password.

4. Firewall Log Configuration and Review

4.1 The firewall will be configured to use system logging.

At a minimum, the firewall log will be configured to detect:

- Alerts, critical conditions, error message and VPN sessions,
- Unsuccessful login attempts
- Logon Access and configuration attempts made to the firewall

5. Firewall Rule Review

5.1 At least quarterly, IT Officer must ensure that a report of all firewall rules that relate to Williamsburgh IP addresses is documented.

5.2 At least quarterly, IT Officer must review all rules that affect its services and ensure that rules still meet the business need.

5.3 All firewall rules that are no longer required or are not essential to the business must be removed or disabled in a timely manner.

5.4 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.

5.5 A Firewall Audit will be carried out annually as part of the Penetration Test that is carried out by an independent Approved Penetration Test Company.

6. Policy Review

6.1 This policy shall be reviewed every year by the Finance and IT Manager and IT Officer to:

- Determine if there have been changes in International, National or Internal references that may impact on this policy.
- Determine if there are major changes to the network requirements.

Appendix 1

Firewall Access Request Form

Requester's Name	Requester's Phone No.	Requester's Email	Department	Username	Date Of Request

Description of what you are trying to accomplish (use additional pages if needed):

Firewall Rule Required:

	Source Address /Subnet Mask	Source Protocol/Port	Destination Address	Destination Protocol/Port	Action: Deny/Allow	Rule: Add/Remove/Modify	Description

The following section is to be completed by IT Officer and Finance/IT Manager:

Request Security Review Results	
Request Results: Approved/Denied, and Comments	
Date:	**Name:**
Date:	**Name:**