# Family First Credit Union
## Firewall Policy

### General Policy Statement:

A firewall is a collection of components (e.g., computers, routers, software) that mediate access between different security domains. All traffic between the security domains must pass through a firewall, regardless of the direction of the flow. The purpose of this policy is to provide management's expectations for how the firewall should function. The firewall selection will be determined by the ongoing security risk assessment process.

### Reference:

National Institute of Standards and Technology (NIST). Special Publication 800-53 (Revision 4) Security Controls and Assessment Procedures for Federal Information Systems.

### Guidelines:

1. **TYPE OF FIREWALL UTILIZED**. There are different implementations of firewalls which can be arranged in different ways. The firewall implementations are discussed below as they would apply to low, medium and high risk processing environments.

    i. **Packet Filter Firewalls**. Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, the firewall drops the packet. These firewalls offer minimum security but at a very low cost, and can be an appropriate choice for a low risk environment. They are fast, flexible, and transparent. Filtering rules are not often easily maintained on a router, but there are tools available to simplify the tasks of creating and maintaining the rules.

    ii. **Application-Level Firewalls**. Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application-level continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc.

Application level firewalls will be configured such that out-bound network traffic appears as if the traffic had originated from the firewall (i.e. only the firewall is visible to outside networks). In this manner, direct access to network services on the internal network is not allowed. All incoming requests for different network services such as Telnet, FTP, HTTP, etc., regardless of which host on the internal network will be the final destination, must go through the appropriate proxy on the firewall. Applications gateways require a proxy for each service, such as FTP, HTTP, etc., to be supported through the firewall.

a) When a service is required that is not supported by a proxy, the Credit Union will do one of the following:

- Deny the service until the firewall vendor has developed a secure proxy; or

- Pass the service through the firewall - using what are typically called "plugs," most application gateway firewalls allow services to be passed directly through the firewall with only a minimum of packet filtering. This can limit some of the vulnerability but can result in compromising the security of systems behind the firewall.

b) When an in-bound Internet service not supported by a proxy is required to pass through the firewall, the firewall administrator will define the configuration or plug that will allow the required service. When a proxy is available from the firewall vendor, the plug must be disabled and the proxy made operative.

c) All in-bound Internet services must be processed by proxy software on the firewall. If a new service is requested, that service will not be made available until a proxy is available from the firewall vendor and tested by the firewall administrator. A custom proxy can be developed in-house or by other vendors only when approved by the Information Technology Manager.

iii. **Hybrid or Complex Gateways**. Hybrid gateways combine two or more of the above firewall types and implement them in series rather than in parallel. If they are connected in series, then the overall security is enhanced; on the other hand, if they are connected in parallel, then the network security perimeter will be only as secure as the least secure of all methods used. In medium to high risk environments, a hybrid gateway may be the ideal firewall implementation.

2. **FIREWALL ARCHITECTURES**. Firewalls can be configured in a number of different architectures, provided various levels of security at different costs of installation and operation. The Credit Union will match its risk profile to the type of firewall architecture selected.

    i. **Multi-Homed Host**. A multi-homed host is a host (a firewall in this case) that has more than one network interface, with each interface connected to logically and physically separate network segments. A dual-homed host (host with two interfaces) is the most common instance of a multi-homed host.

    For instance, one network interface is typically connected to the external or untrusted network, while the other interface is connected to the internal or trusted network. In this configuration, a key security tenet is not to allow traffic coming in from the untrusted network to be directly routed to the trusted network - the firewall must always act as an intermediary. Routing by the firewall will be disabled for a dual-homed firewall so that IP packets from one network are not directly routed from one network to the other.

    ii. **Screened Host**. A screened host firewall architecture uses a host (called a bastion host) to which all outside hosts connect, rather than allow direct connection to other, less secure internal hosts. To achieve this, a filtering router is configured so that all connections to the internal network from the outside network are directed towards the bastion host. If a packet filtering gateway is to be deployed, then a bastion host will be set up so that all connections from the outside network go through the bastion host to prevent direct Internet connection between the Credit Union network and the outside world.

    iii. **Screened Subnet**. The screened subnet architecture is essentially the same as the screened host architecture, but adds an extra strata of security by creating a network which the bastion host resides (often called perimeter network) which is separated from the internal network. A screened subnet will be deployed by adding a perimeter network in order to separate the internal network from the external. This assures that if there is a successful attack on the bastion host, the attacker is restricted to the perimeter network by the screening router that is connected between the internal and perimeter network.

3. **PHYSICAL PLACEMENT OF THE FIREWALL COMPONENTS**. Physical access to the firewall will be tightly controlled to prevent any authorized changes to the firewall configuration or operational status, and to eliminate any potential for monitoring firewall activity. In addition, precautions will be taken to ensure that proper environment alarms and backup systems are available to assure the firewall remains online. The Credit Union's firewall will be located in a controlled

environment, with access limited to the firewall administrator.

The room in which the firewall is to be physically located will be equipped with heat, an air-conditioner, and smoke alarms to ensure the proper working order of the room. The placement and recharge status of the fire extinguishers will be checked on a regular basis. If uninterruptible power service is available to any Internet-connected systems, such service will be provided to the firewall as well.

4. **FIREWALL ADMINISTRATION**. A firewall, like any other network device, has to be managed by someone. A firewall administrator will be designated by the Information Technology Manager and will be responsible for the upkeep of the firewall.

    i. **Remote Firewall Administration**. The most secure method of protecting against attacks is to have strong physical security around the firewall host and to only allow firewall administration from an attached terminal. However, operational concerns often dictate that some form of remote access for firewall administration be supported. In no case will remote access to the firewall be supported over untrusted networks without some form of strong authentication. In addition, to prevent eavesdropping, session encryption will be used for remote firewall connections.

        a) **Low Risks**. Any remote access over untrusted networks to the firewall for administration must use strong authentication, such as one time passwords and/or hardware tokens.

        b) **Medium Risks**. The preferred method for firewall administration is directly from the attached terminal. Physical access to the firewall terminal is limited to the firewall administrator and backup administrator. Where remote access for firewall administration must be allowed, it should be limited to access from other hosts on the Credit Union's internal network. Such internal remote access requires the use of strong authentication, such as one time passwords and/or hardware tokens. Remote access over untrusted networks such as the Internet requires end to end encryption and strong authentication to be employed.

        c) **High Risks.** All firewall administration must be performed from the local terminal - no access to the firewall operating software is permitted via remote access. Physical access to the firewall terminal is limited to the firewall administrator and backup administrator.

    ii. **User Accounts**. Firewalls will never be used as general purpose servers. The only user accounts on the firewall will be those of the firewall administrator.

In addition, only the firewall administrator will have privileges for updating system executables or other system software. Only the firewall administrator and the Information Technology Manger will be given a user account on the Credit Union's firewall. Any modification of the firewall system software must be done by the firewall administrator and requires approval of the Information Technology Manager.

iii. **Firewall Backup**. To support recovery after failure or natural disaster, a firewall like any other network host has to have some policy defining system backup. Data files, as well as system configuration files, need to have a backup plan in case of firewall failure. The firewall (system software, configuration data, database files, etc.) will be backed up daily, weekly, and monthly so that in case of system failure, data and configuration files can be recovered. Backup files will be stored securely on a read-only media so that data in storage is not over-written inadvertently and locked up so that the media is only accessible to the appropriate personnel.

5. **UPDATING**. To prevent unauthorized modifications of the firewall configuration, some form of integrity assurance process will be used. Each time the firewall configuration has been modified by the firewall administrator, it is necessary that the system integrity online database be updated and saved onto a file system on the network or removable media. If the system integrity check shows that the firewall configuration files have been modified, it will be known that the system has been compromised. The firewall's system integrity database will be updated each time the firewall configuration is modified. System integrity files will be stored on read only media or off-line storage. System integrity will be checked on a regular basis on the firewall in order for the administrator to generate a listing of all files that may have been modified, replaced, or deleted.

6. **DOCUMENTATION**. The operational procedures for a firewall and its configurable parameters will be documented, updated, and kept in a safe and secure place. This assures that if the firewall administrator resigns or is otherwise unavailable, an experienced individual can read the documentation and rapidly pick up the administration of the firewall. In the event of a break-in such documentation also supports trying to recreate the events that caused the security incident.

7. **INCIDENT RESPONSE**. The firewall will be configured to log all reports on daily, weekly, and monthly bases so that the network activity can be analyzed when needed. Firewall logs will be examined on a weekly basis to determine if attacks have been detected. The firewall administrator shall be notified at any time of any security alarm by email, pager, or other means so that he may immediately respond to such alarm. The Credit Union will follow its Incident Response Policy to address incidents of unauthorized access to member information.

8. **REGULAR AUDITING**. Most firewalls provide a wide range of capabilities for logging traffic and network events. Some security-relevant event that will be recorded on the firewall's audit trail logs are: hardware and disk media errors, login/logout activity, connect time, use of system administrator privileges, inbound and outbound e-mail traffic, TCP network connect attempts, in-bound and out-bound proxy traffic type.

9. **CONTINGENCY PLANNING**. Once an incident has been detected, the firewall may need to be brought down and reconfigured by Members Core Alliance (Firewall Vendor). If it is necessary to bring down the firewall, Internet service will be disabled or a secondary firewall will be made operational - internal systems will not be connected to the Internet without a firewall. After being reconfigured, the firewall must be brought back into an operational and reliable state. In case of a firewall break-in, the firewall administrator will be responsible for reconfiguring the firewall to address any vulnerabilities that were exploited. The firewall will be restored to the state it was before the break-in so that the network is not left wide open. While the restoration is going on, the backup firewall will be deployed.