Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Firewall Policy:

PURPOSE:

The Clarendon College gateways are protected by external firewalls between the Internet and the Clarendon College network to establish a secure environment for the College's information technology resources. Internal firewalls are in place to establish secure communications between different segments of the College's network where various levels of security are warranted. Firewalls are enabled and configured on servers and workstations attached to the college's internal network.

Clarendon College's firewalls are key components of the College's network security architecture. The Firewall Policy governs how firewalls filter traffic to mitigate the risks and losses associated with security threats to Clarendon College's information technology resources. This policy will attempt to balance risks incurred against the need for access.

This policy aims to protect Clarendon College's information technology resources from hacking and virus attacks by restricting access to information technology resources on the College campus. It is designed to minimize the potential exposure of Clarendon College to the loss of sensitive, confidential data, intellectual property, and damage to the public image, which may follow from unauthorized use of Clarendon College's information technology resources.

SCOPE:

The Firewall Policy applies to all firewall devices owned and/or operated by Clarendon College.

POLICY STATEMENT:

Perimeter Firewalls:

The perimeter firewall permits the following outbound and inbound Internet traffic:

1. *Outbound* - All Internet traffic to hosts and services outside Clarendon College's networks except those specifically identified and blocked as malicious sites.
2. *Inbound* - Allow Internet traffic that supports the institution's mission by defining system, application, and service procedures.
3. *Outbound/Inbound* – All internet traffic detected as malicious by the College's intrusion prevention system (IPS) and/or all traffic violating Clarendon College firewall policies is dropped.

Reason for filtering ports:

1. Protecting Clarendon College Internet Users - Certain ports are filtered to protect Clarendon College's information technology resources. The perimeter firewall protects against certain common worms and dangerous services on Clarendon College information technology resources that could allow intruders access.

2. Protecting our outbound bandwidth - If Clarendon College Internet users overuse their outbound bandwidth by running high-traffic servers or by becoming infected with a worm or virus, it can degrade the service of other Clarendon College systems.
3. Protecting the rest of the Internet - Some filters prevent users from knowingly or unknowingly attacking other computers. In addition to being in Clarendon College's interest in protecting our bandwidth, it is the institution's responsibility to prevent abuse of its network.

Roles and Responsibilities:

The Information Security Office is responsible for implementing, configuring, and maintaining Clarendon College's firewalls and activities relating to this policy.

1. At a minimum, firewalls must be annually tested and reviewed.
2. When there are significant changes to the network requirements, firewall security policies will be reviewed and may warrant changes.
3. Firewalls must have alert capabilities and supporting procedures.
4. Auditing must be active to permit analysis of firewall activity.
5. All firewall changes will be documented.

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Firewall: This is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

Gateway: This is the computer or device that routes the traffic from a workstation to the outside network serving the Web pages.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology.
The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.