

TITLE: Firewall Use Policy

Category: Technical Support	
Original Effective Date: 3-12-08	Review Date: February 2008

Due to ACCEL systems' required connection and access to the public Internet, it is essential that a strong perimeter firewall exists that sufficiently separates the internal private LAN/WAN of ACCEL systems and the public Internet. Barton, as the technology support center for ACCEL, will utilize firewall technology, as appropriate to protect information systems and clinical information also referred to as electronically protected health information or EPHI.

Firewall technology utilized by Barton to protect ACCEL systems have the following characteristics:

1. Allow for filtering of communication protocols based on complex rule sets.
2. Provide extensive logging of traffic passed and blocked.
3. All inbound and outbound traffic to the public Internet from the ACCEL systems' LAN/WAN must pass through the firewall.
4. It is sufficiently hardened to resist internal and external attacks.
5. Fails closed and deny all traffic once closed.
6. Does not disclose the internal nature, names, or addressing of the ACCEL systems' LAN/WAN.

Firewall Physical Location

Firewall components are located in secured areas within Barton's IS Dept to which only authorized Barton IS staff have appropriate access. Only Barton Staff may use the direct connection ports on Firewall components. Barton IS staff is responsible for maintaining an accurate inventory of the Firewall components.

Authorization

Authorization to access Firewall components is restricted to BARTON IS personnel with administrative responsibilities. Barton IS management approves administrative authorization based on job responsibilities.

All data traveling between the LAN/WAN and External Networks must pass through the ACCEL systems Firewall. Modems are the only devices that may communicate with an External Network without passing data through the Firewall. Modem usage is extremely restricted.-

Access to external resources located on External Networks may require modification to the Firewall components. When this type of access is required, Authorized Users requiring access to such resources must have an approved business need as approved by Barton IS management

Change Management

Only authorized Barton IS staff will perform the following tasks related to Firewall components:

- Install, upgrade and remove
- Install software and relevant patches and fixes
- Perform hardware maintenance
- Maintain administrator user ids
- Implement appropriate firewall rule changes

Barton will formally document and maintain Firewall component configurations. Barton will store backups of configuration files.

Monitoring

Barton IS staff will evaluate Firewall software upgrades, patches and fixes on a regular basis. If an upgrade/patch/fix is available, Barton IS staff will determine if it is applicable to the ACCEL Systems environment. Authorized Barton IS staff will review and approve each upgrade/patch/fix prior to installation. Barton IS staff will install necessary security-related upgrades/patches/fixes in a timely manner.

Authorized Barton IS staff will monitor Firewall component logs for performance, security and operational events.