

# Security *General Security Guidelines*

QuadData Solutions (QDS) employs many methods to secure your data. The end-result? Peace of mind.

## Physical

- QDS maintains physical security through a variety of methods. Primarily, general admission to any Quad facility is obtained only through authorized entrances. All visitors must check in and wear clearly visible identification indicating their status as such. All other entrances are protected by card access systems.
- Admission to any Quad data center is through card access only, restricted to those Quad individuals in the Information Technology department who require access. All access via card systems is logged and reported regularly. Upon the dismissal or resignation of any Information Technology employee, access is revoked centrally, and that revocation is instant and global for any Quad facility.

## Passwords

QDS maintains secure access to all corporate information systems. All systems are protected by a unique user name and password challenge. Passwords are required to be changed regularly, and must be longer than six characters. Invalid login attempts are restricted to five attempts, and then the account is locked out until reset.

## Firewall/Internet Access

Quad realizes the value and productivity Internet access allows for customers and employees. However, Quad takes security seriously given the dangers of connecting our network to a public forum such as the Internet.

All of Quad's many Internet connections are protected by highly available, load-balanced and fault-tolerant firewall systems, operating with hardened operating systems and best-of-breed, commercially available firewall software solutions. All internal server systems are prevented from using direct Internet access. All Internet access inbound is allowed only to DMZ areas and systems, and only on a per-port, as needed basis. All end-user computers inside of Quad utilize proxy server systems with full logging and authentication. All firewall logs are monitored and documented.

## Audits

Quad's data security staff conducts regular and unannounced audits to check systems for potential security risks, vulnerabilities and threat assessment. Also, to ensure customer and corporate data is as secure as absolutely possible, Quad's information technology systems are audited on a regular basis by independent third party contractors.

## Virus Protection

All servers, e-mail systems and end-user workstations are protected by commercially available virus detection and inoculation systems and software. Virus definition files are checked, and if needed, updated once every hour of every day to ensure all data is free of malicious code. All files attached to either inbound or outbound electronic mail are scanned at the network perimeter, and any offending attachments are removed and notification forwarded to the sending and receiving parties.

## Remote Access

- While realizing that remote access is a requirement of commerce, Quad relies on stringent policies to protect all systems and data in relation to remote access. Any network having a direct connection to Quad for any reason is secured using industry best practices and policies. All customer direct connections are secured via router policies, firewalls and/or both, and are set for the highest level of security, and are regularly monitored and audited.
- Remote user access such as VPN and dial-up access is restricted to only such individuals where access is deemed appropriate. All individuals having such access must first petition for it, and access is contingent on the end-user workstation meeting Quad corporate security requirements for operating system patches and security. All remote access is authenticated via RADIUS systems, and all access is accounted for and logged. In circumstances where it so warrants, filters, firewalls and routing policies are also inserted for VPN remote access users to prevent access to certain hosts, networks or applications via any method.

### QDS' Data Centers

QDS maintains geographically diverse, load-balanced and fault-tolerant data centers, in both West Allis and Sussex, Wisconsin. Each data center is state-of-the-art, and features redundant UPS and power distribution systems, natural gas and diesel generators, redundant environmental systems, as well as highly secured access.

All Quad data centers feature fire suppression systems of either dry-pipe water, or Halon, and a multitude of sensors for heat, smoke, water and humidity.

### Contingency Planning

- QDS safeguards data many ways. As stated earlier, to ensure availability and near-instantaneous fail-over, Quad maintains two load balanced and fault-tolerant data centers in southeastern Wisconsin.
- Back-up copies of all system information are sent to tape via large scale automated backup systems. Quad maintains three automated storage silos. These silos are located in Sussex, West Allis and Hartford, Wisconsin. All corporate and customer data is transferred from online systems to tape nightly across Quad's global network to one of these facilities, resulting in nightly backups and instant off-site storage.

### Network Diversification

To maintain as close to 99.999% availability as possible, Quad employs a strict policy of carrier, route, demarcation point and egress point diversity. All broadband circuits that provide service to Quad's global network are routed and diversified in such a way as to never have a single point of failure in any facility. All servers, where applicable, feature dual network connections, and every print production, imaging, and sales location features at least two and sometimes many more network technologies, carriers, circuits and equipment to guarantee availability in the event of a failure.