

Information Technology Security Procedures



NETWORK SECURITY OVERVIEW

These procedures establish security requirements to ensure that the exchange of confidential and sensitive information among computing systems via attached networks are secure, as required by the Information Technology Security Program. All HIPAA, FISMA, and GLBA compliant servers within the ResponsiveWeb Network, interconnecting links, remote connectivity links (including wireless connections), and connections to public and other private networks within the control and authority of ResponsiveWeb are subject to these procedures.

BACKGROUND

Data networks at the ResponsiveWeb Datacenter are connected to provide routine communications:

- a. within ResponsiveWeb's Network
- b. between ResponsiveWeb servers and other ResponsiveWeb Components
- c. to remote sites, including but not limited to those of Hospital and Clinic affiliations, collaborating Institutions, vendors, and contractors; and
- d. to public networks, including the Internet.

PROCEDURE

All potential points of network accessibility must be protected with the same level of network security. All information resources will be protected by varying levels of security by the firewall system, depending on their compliance classification.

1. All network equipment, including routers, switches, concentrators and hubs, connected to the ResponsiveWeb Network will be authorized by the IT Security Core (ITS Core) team, or its designees.
2. Only devices approved by the ITS Core, or its designees may provide domain name service (DNS), dynamic host configuration protocol (DHCP), network time protocol (NTP) or dynamic routing services. These services are classified as critical network information or services and are restricted to approved machines only.
3. Network computing devices such as workstations, and servers hosting file-sharing, print-sharing or multiple-user applications must be approved by the

ITS Core, or its designees, to prevent unauthorized network connections.

The ITS Core should be notified biannually as to the number of PCs, laptops, wireless devices and palm pilots (PDA) on each network segment.

- 4. All collocated and on site connected devices at the ResponsiveWeb Datacenter must meet minimum security configuration requirements. The device owner is responsible for keeping the device up to date with required patches, and if incapable or unwilling must designate an individual to assume this responsibility, however, accountability remains with the device owner.**
- 5. Remote links to or from the ResponsiveWeb Network must be approved by the ITS Core, or its designees. These links include but are not limited to Virtual Private Networks (VPN), analog modems, and wireless hubs or switches, synchronous and asynchronous leased lines. All such devices must be registered with the ITS Core. Audit logs must be maintained including time, date, remote user and devices accessed. Logs must be reviewed to detect anomalies.**
- 6. All networks will be monitored by the IT Infrastructure Owners for unauthorized traffic, including penetration attempts and denial of service attacks. Traffic monitors and recorders, if any, including sniffers, protocol analyzers, keystroke analyzers, etc. will be used only by personnel approved by the ITS Core.**
- 7. If high levels of activity causing network problems are detected on any of the network zones, network operations personnel are able to trace the activity through the network to the workstation that is causing the activity. If suspicious activity is detected and the Client responsible for the server is not available, the IT Infrastructure Owners may disable that particular server**

from the network for the security of the Client, and ResponsiveWeb. The Client in charge of the server or subnet will be contacted as soon as possible. If the occurrence is during weekend hours, the Client will be contacted the next business day. Incident response activities will then commence.

8. All patient information (including but not limited to demographic, financial and clinical data) transmitted via email or transmitted on networks outside of the ResponsiveWeb Network internal zones will be encrypted. All patient information stored within ResponsiveWeb Network internal zones will be encrypted where applicable. The ResponsiveWeb Network will use appropriate encryption technology systems approved by the ITS Core. The encryption protocol must ensure the integrity of the information being transmitted and stored.
9. Users requiring access to network information resources, including servers, workstations, and network equipment must have individual user-ids using accounts that require acceptable authentication.
10. Access to network information resources with confidential information requires the application of the following stringent security controls:
 - Physical Security
 - Host and Server Configuration
 - User Authentication
 - User Authorization
 - Encryption
 - Intrusion Detection
 - Incident Reporting

11. **If unauthorized access or modification of confidential data occurs, the ITS Core will be promptly notified and the incident will be documented. Appropriate corrective actions will be planned for and established to minimize or eliminate the possibility of recurrence.**
12. **The ResponsiveWeb Network Infrastructure is protected by fire life safety and smoke purge systems, as well as 24-hour attended lobby and security force with integrated CCTV and Card Access Systems. Building systems, perimeter and sensitive areas are monitored 24/7 from a Security Station located on Ground Floor.**
13. **To support the designed power consumption and all ancillary loads, we utilize 128 (130-ton) dry coolers and similar piggyback units.**
14. **Servers will be distributed spatially to never consume more than 100 watts per square foot of power at 480 volts, 3-phase, 4 wire. Existing electric service consists of three 2,000-kVA, 460V, 3-phase transformers. New infrastructure design consists of four vaults, each capable of housing six 2,500-kVA transformers, providing 52,500 kVA of total power or roughly 13,000 kVA per vault at 480 volts. ConEdison has the ability to serve the total planned requirements of the building. ResponsiveWeb's Network is served by ConEdison's N+ 2 redundant design format for all phases of power distribution.**
15. **A dedicated generator farm has been master planned to accommodate 31 (2,000-kw) generators and ancillary equipment for standby back-up power to guard against interruptions or low voltage conditions. Depending on power requirements, these generators are available through paralleling gear, or standing alone for a specific user or multiple users.**

16. The ATC has been master planned to accommodate fuel storage and containment and associated pumping and filtering stations for approximately 300,000 gallons of diesel fuel. This will provide tenants with sufficient fuel storage capacity to operate all generators on a continuous basis for 72+ hours without refueling.

WWW.RESPONSIVWEB.COM

OPERATOR@RESPONSIVWEB.COM

RESPONSIVWEB LLC OFFICES IN THE AMERICAS

UNITED STATES – EDISON, NJ

CORPORATE HEADQUARTERS

PHONE: + 1 888 RW2 HOST x23

UNITED STATES – FRANKLIN PARK, NJ

PHONE: + 1 888 RW2 HOST x33

the responsiveweb logo is a trademark of responsiveweb llc

all other products referenced are the service marks of the respective owner.

© 2007, responsiveweb llc

all rights reserved | printed in the usa