NEW YORK STATE THRUWAY AUTHORITY
NEW YORK STATE CANAL CORPORATION

NETWORK CONNECTION REQUIREMENTS

A. Permissible Access

The Authority will limit access to a Network Connection to those services and devices (hosts, routers, etc.) needed. Blanket access will not be provided.

The Authority does not allow a Network Connection to be used as Outside Entity's Internet connection.

B. Connectivity Options

The following connectivity options are the standard methods of providing an Outside Entity with an external connection to the Authority's data communications network ("Network Connection"). Anything that deviates from these standard methods must be approved in advance by the Authority.

1) Encrypted Tunnel – The preferred connectivity method is via the Internet to an Authority Virtual Private Network (VPN) device. The Authority may loan Outside Entity, in accordance with the Outside Entity Equipment Loan Agreement, the required client software for establishing VPN connections with the Authority. The Authority's perimeter security measures will control access to the internal network.
2) NYeNet/MAN Connection – This can include a VPN.
3) Leased Circuit.
4) Fiber.
5) Dial-in.

C. Authentication of Network Connection

Outside Entity must authenticate its Network Connection using Authority authentication systems. All Outside Entity remote access user accounts will have an expiration time consistent with the business justification for the access, which can be renewed at the discretion of the Authority. If the term of the Network Connection is longer than one year, then Outside Entity must generate a report at least once per year showing which Outside Entity employees have access to the Network Connection and send such report to the Authority for verification and review. Further, any time there is a change in those Outside Entity employees who have access to the Network Connection, Outside Entity shall send the Authority an updated list of those Outside Entity employees who have such access.

D. Current Software Versions Required

Outside Entity must, for all computers it utilizes for a Network Connection, employ software versions that are currently supported by the software manufacturer. Outside Entity must apply all available security updates and hot fixes for that software in a timely fashion.

All Outside Entity software and firmware utilized for a Network Connection must be kept up to date, especially with patches that fix security vulnerabilities.

E. Virus Protection

Outside Entity must install and enable anti-virus software on all computers utilized for a Network Connection and keep such virus definition files up to date.

F. Protection of Authority Information and Resources

The Authority will implement all security measures it determines appropriate to protect the integrity and confidentiality of Authority confidential information.

The Authority will implement appropriate "Access Control Lists" (ACLs) on the Authority network devices to which the Outside Entity sites are connected. The ACLs will restrict access to pre-defined hosts within the internal Authority network.

In the event the Authority agrees to loan to Outside Entity certain Authority equipment and/or software ("Authority-owned Equipment") to facilitate the Network Connection, the Authority will provide Outside Entity with enable-level access only to those Outside Entity employees necessary to the installation, operation and maintenance of the Network Connection. All other Outside Entity employees will have restricted access/read-only access to the routers at their site and will not be allowed to make configuration changes.

Outside Entity shall be solely responsible for providing the appropriate security measures to ensure protection of its internal network and information. The Authority shall not have any responsibility for ensuring the protection of Outside Entity information.

G. Security Incident Notification and Resolution

Outside Entity is responsible for notifying the Authority upon discovery of any security incident that may threaten or compromise the confidentiality, integrity or availability of Authority information or network infrastructure. Outside Entity shall, at a minimum, report the following to the Authority: 1) successful or unusually persistent attempts to gain unauthorized information or system access; 2) presence of malicious code that has a widespread impact throughout Outside Entity's network infrastructure; 3) a known or suspected denial of service attack; and 4) scans and probes that precede or are related to a security incident listed above.

Once it has resolved the security incident, Outside Entity must also report the following to the Authority: 1) attack source details (i.e., IP address, method, vulnerability exploited, etc.); 2) the specific effects (i.e., loss, damage, destruction, modification, disclosure) on systems, accounts or information assets resulting from the threat or compromise; and 3) actions taken to remediate the security incident.

NEW YORK STATE THRUWAY AUTHORITY
NEW YORK STATE CANAL CORPORATION

H. Audit and Review of Outside Entity Network Connections

The Authority shall have the right at all times to monitor all aspects of Network Connections. The Authority will employ automated tools to accomplish monitoring tasks where practicable. The Authority will generate an annual report on its authentication database showing the specific Outside Entity login entries and distribute such reports to appropriate Authority personnel for review. The Authority will periodically audit Network Connections and distribute such audits to appropriate Authority personnel for review.

The Authority will review all Network Connections on an annual basis and update or terminate such connections when appropriate.