Security Architecture Standard

Purpose

Information security must be an integral and mandatory part of any system or infrastructure designed to provide access to information. It is very difficult to add information security measures after a system has been designed, and the resulting system may not comply with City of New York Information Security policies. This document will define various models and security controls so that a system can be built to interface with the existing architecture.

Scope

All externally accessible applications and internally accessible multi-agency applications developed to support City of New York business must be built in a secure fashion. These applications must be reviewed and approved by the Citywide Chief Information Security Officer (CISO). Accreditation must be achieved prior to migrating to the production environment.

Background

CityNet is a Department of Information Technology and Telecommunications (DoITT) operated, trusted network that interconnects city agencies, hosts citywide applications, and provides Internet-based services citywide. DoITT utilizes policies, processes, and technology to protect this network, its applications, its hosts, and the data processed therein. This layered security design comprises the CityNet Security Architecture.

Security Policy

The Citywide Chief Information Security Officer (CISO) has responsibility for ensuring appropriate security controls are applied to protect the confidentiality, integrity, and availability of City of New York information systems.

The purpose of Citywide Information Security Policies is to provide guidance for selecting and specifying appropriate security controls for information systems. These policies have been developed to:

- Facilitate a more consistent, comparable, and repeatable approach for selecting and specifying security controls for City systems;
- Facilitate development of Citywide baseline security controls for information systems based on the confidentiality, integrity, and availability requirements;
- Create a foundation for the development of information system security controls that meet legal requirements, industry best practices, and City objectives;
- Facilitate the development of consistent assessment methods and procedures for testing security controls effectiveness.

Data Classification

The Data Classification Policy provides a critical foundation for information security decisions. To ensure that business information assets receive an appropriate level of protection, the value

of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

All information at the City of New York and corresponding agencies will be classified at one of four levels: Public, Sensitive, Private, or Confidential.

Public	This information might not need to be disclosed, but if it is, it shouldn't cause any damage.
Sensitive	This information requires a greater level of protection to prevent loss of confidentiality.
Private	This information is for agency use only, and its disclosure would damage the reputation of the agency.
Confidential	This is the highest level of sensitivity, and disclosure could cause extreme damage to the agency.

When looking at the information stored or processed by an application, it is important to assess its classification based on the content itself, where it was collected, where it will be stored, the method of transmission, and how it will be queried.

For example, a name or address may be publicly available information. If it was collected by a HIPAA application, and is stored in a shared database with other application data that can tie the name to a medical condition, the classification changes. The Citywide Chief Information Security Officer will use this context as part of his decision making.

Security Accreditation Process

All externally accessible applications and internally accessible multi-agency applications developed to support City of New York business must be built in a secure fashion. These applications must be reviewed and approved by the Citywide Chief Information Security Officer (CISO). Accreditation must be achieved prior to migrating to the production environment. See the "Security Accreditation Process**"** document for more information.

Security Zones

CityNet is logically divided into security zones, where corresponding security controls are defined based on security policy, threats and exposure:

Untrusted	Systems that are unmonitored and unprotected by DoITT security infrastructure.
DMZ	Systems that are protected and monitored by DoITT security infrastructure, but have some direct exposure to the Internet.
Trusted	Internal systems that are part of shared service environments and are protected and monitored by DoITT security infrastructure.
Most Trusted	Internal LAN segments, connected to CityNet, without any external connections that are protected by firewalls.

Perimeter

A traditional information security paradigm is the "perimeter." The perimeter logically demarcates between the uncontrolled Internet and internal networks that fall under some level of DoITT control. The CityNet perimeter is defined by the following touch points:

- Redundant Internet connections
- Extranet points of presence connected to CityNet
- Site to Site VPN Connections
- NYCWiN wireless infrastructure
- Out of band connections

Internet Access

All outgoing Internet access must be authenticated, monitored, filtered, and tracked. For authentication, individual agencies may pass their local Internet traffic through an agency proxy. Agencies may also use the shared proxy servers in the hosting environment. DoITT also maintains a content filter service at the perimeter, which forces all traffic through a content filter to block inappropriate and dangerous internet access. The content filter also controls access for those users who are restricted to viewing specifically authorized websites. The content filter also plays a key role in blocking access to websites that host malicious code used to infect PCs. Agency heads who chose to opt out of the DoITT managed content filter and deploy a local filtering solution will certify to the Citywide CISO and the Inspector General for their respective agencies that a localized content filter is in place.

NOTE: The Department of Investigation's Inspector General may request these logs in hard or electronic format in support of an investigation.

City agencies **may not** maintain direct connections to the Internet or to any external entities on any CityNet connected device. Connection via the DoITT-supported CityNet cloud, or otherwise, is granted only upon review culminating in approval. DoITT is properly configured to act as a City agency's high-bandwidth Internet service provider (ISP) and VPN/extranet provider.

DoITT also maintains an Anti-Spyware system that blocks access to known malware and spyware sites and traffic. This system detects the traffic in a similar fashion to an IDS and then resets the connection before it can reach the Internet.

CityNet Connectivity

There are eight main connectivity models that are supported by DoITT:

1) Direct Agency connectivity – The most common CityNet connections are those between the Agencies and CityNet. These connections are facilitated through DoITT routers at key locations throughout the City of New York. There are no access controls on these routers.
2) ISP Agency connectivity – There are some agencies that maintain their own connections to the Internet as well as connections to CityNet. These agencies are separated from CityNet by a firewall since DoITT does not control these ISP connections and cannot maintain the integrity of CityNet without this control.

3) Extranets (site to site connections via dedicated connections) – These include partners such as financial institutions, that maintain dedicated connections (for example, T1) to City financial systems.
4) VPN Connections (site to site connections via the Internet) – These include partners such as financial institutions, that require persistent connections to City financial systems. These connections are supported through site to site IPSec VPN tunnels that terminate on the Internet perimeter. DoITT supports a VPN "Edge" device for smaller remote offices that may not have IPSec capable perimeter equipment.
5) Application specific connections – When an external vendor or business partner needs access to a specific extranet or internal application, this access is provisioned through SSL VPN. The SSL VPN allows external parties to connect to DoITT via their standard web browser, eliminating the need for a heavy client to be installed on their workstation. This access type is also used for applications that need to be exposed to a known set of external users.
6) General purpose remote access – DoITT provisions SSL VPN profiles for employees who need remote access for "telework."
7) Client to server connections – When a vendor or other entity needs access to a system that is difficult to support via SSL VPN, client IPSec connections can be used.
8) Government extranet connections – Government extranet connections such as those from NYS terminate in a dedicated DMZ.

DoITT maintains VPN tunnels to many partners. CityNet is not to be used to facilitate pass-through connectivity between VPN-connected agencies and other remote resources.

ISP Agency connectivity through the Citywall firewalls is designed to facilitate a controlled subset of traffic exchange. If an agency desires to take advantage of the full offering of DoITT managed services, such as email, server, and desktop support, it must first remove its ISP connection and become an integrated CityNet Agency.

Remote Access

Agencies are strongly encouraged to use a dedicated terminal server on their network for access to non-web applications.

A prerequisite for both modes of client VPN are an agency directory such as LDAP or Active Directory. DoITT remote access solutions do not support locally configured user databases.

Site to Site VPN should be used whenever an organization needs a persistent connection to CityNet. The tunnel will be limited with firewall rules to allow them minimum access needed to accomplish business related tasks. Site to site VPN is also the recommended method for allowing external groups of support personnel or developers from a single organization to access CityNet.

IPSec tunnels used within CityNet may not traverse firewalls. For special situations where internal tunnels are required and must traverse a firewall, they must be terminated on both ends of the boundary to allow for inspection of the encapsulated traffic.

SSL VPN (RA) is the recommended method of remote access. It uses SSL as the tunneling mechanism, which is almost universally allowed through firewalls. For access to

internal, web based applications, it is also clientless.

DMZ

A DMZ is a set of logical networks with direct access to the Internet as well as internal networks. It acts as a buffer between the untrusted Internet and trusted internal networks, allowing select services to be exposed to the Internet while not doing so directly from trusted areas. The following general requirements apply to all City DMZs:

1) Traffic originating from Internet based systems must be authenticated at the perimeter before being allowed to access CityNet.
2) Databases may not be placed within the Internet DMZs.
3) Groups that require administrative access to servers within any DMZ may do so only with pre-approved workstations.
4) Applications developed primarily for internal users with a limited external user base will not be exposed to the Internet and will use VPN for access.

Internal CityNet Firewalls

There are two models for the use of firewalls on CityNet. 1) Many agencies maintain firewalls between CityNet and their agency network. In this scenario, they are completely responsible for any troubleshooting or impact that it might have on their interactions with CityNet. 2) For systems deployed on CityNet designed to support multiple agencies that process PRIVATE information, a firewall has been implemented to logically keep unauthorized traffic from impacting that environment.

Security Monitoring

DoITT maintains a number of monitoring tools that collect and analyze information that moves across CityNet.

- Network – Intrusion detection (IDS) and behavior analysis tools collect information from the network through direct observation and Netflow statistical analysis.
- Event Based – Security information and event management (SIEM) tool collects log events from firewalls.
- Host Based Intrusion Prevention Agents collect information on unauthorized changes made to systems.

Email Protection

DoITT maintains redundant email gateway infrastructures that provide anti-spam and anti-virus protection for email that flows through CityNet.

Enterprise Directory Services

DoITT maintains an Enterprise LDAP directory service that provides centralized authentication services and Agency directory interoperability. This service should be used for all authentication and authorizations needs. Application specific and proprietary credential stores are strongly

discouraged.

Telephony

Citywide Telephony Services are physically located behind firewalls in order to prevent unauthorized access.

Digital Certificates

Digital certificates play a key role in effective deployment of SSL based technologies and PKI. DoITT maintains an internal certificate authority for the provisioning and revocation of internally used certificates. DoITT facilitates the procurement of 3rd party certificates for publicly facing applications.

Document Revision History

Date	Description
September 27, 2012	**Version 1.9-E** Initial publication of Public document.