CISO Role

The Policy

The Chief Information Security Officer (CISO) or agency designee has a leadership responsibility for protection of agency information assets.

Background

The Chief Information Security Officer (CISO) is the focal point for all information resource protection matters within each Agency. The CISO is the agency leader responsible for promoting information security within the agency. The CISO or appropriate agency designee has responsibility for ensuring compliance with City of New York, Citywide Information Security Policies.

CISO Responsibilities

1) Partnering with agency employees and consultants to ensure understanding of and adherence to the Citywide Information Security Policies.
2) Promptly reporting security incidents or significant security problems to appropriate personnel within the Agency, and to DoITT where the incidents or problems implicate or affect Citynet.
3) Acts as an advisor to the Agency CIO (or equivalent position) regarding Agency compliance with the Citywide Information Security Policies. This requires that the CISO either report directly to the Agency CIO (or equivalent position), or have direct access to the Agency CIO (or equivalent position) when necessary.
4) Keeping up to date on information security topics regular, CISO conferences, and teleconferences sponsored by DoITT and other recognized information security organizations, i.e. SANS, ISSA, ISACA, etc.

Security Governance

5) Establishing procedures to ensure that systems and/or software comply with the Citywide Information Security Policies.

Training and Awareness

6) Overseeing the establishment and execution of information security training for the agency.
7) Being the leader in promoting information security into all appropriate agency business plans and overseeing execution, and especially ensuring that Agency Information Owners understand and execute their responsibilities appropriately.
8) Establishing an information technology security awareness program to ensure all department employees understand and adhere to information technology policies and standards.

Mission and Mandate Development

9) Coordinate closely with those responsible for physical security within their respective Agency.

10) Continuously identifying, updating and maintaining information regarding potential security vulnerabilities, risk and threats to the enterprise information technology infrastructure, and distributing technology security information to appropriate staff.

11) Provide instructions and coordination regarding software configuration standards for servers and desktop systems that are or may be attached to the enterprise network where necessary to ensure information technology security.

12)

Document Revision History

Date	Description
September 7, 2007	**Version 1.0** Issued
June 16, 2011	**Version 1.1** Updated header with new NYC logo and added this revision history table to the document.
April 19, 2012	**Version 1.2** Changed classification of this policy from sensitive to public.