Metropolitan Council

POLICY – INFORMATION SECURITY

Section/Number:	3-6 Information Security Policy	Total Pages:	2
Dept. Responsible:	Information Services	Effective Date:	to be determined
Special Note:	This policy supersedes previous information security policies	Revision No	

I. Policy:

Information and systems belonging to the Metropolitan Council must be managed and protected so that confidentiality is maintained (preventing information from unauthorized disclosure), integrity is ensured (preventing information and systems from accidental and malicious modification), and availability is guaranteed (ensuring the reliability and accessibility of data and resources to authorized individuals in a timely manner).

Any activities that may damage information or the IT infrastructure belonging to the Metropolitan Council, or harm the Council's image, are prohibited. This includes, but is not exclusive to, circumventing security measures, taking advantage of weaknesses, infringing on copyrights, cracking passwords, and accessing information without authorization. All information must be protected against unauthorized access in line with the respective security requirements.

II. Purpose of policy:

The Metropolitan Council Information Security Policy governs fundamental aspects relating to information security at the Metropolitan Council for the protection of the Council, its employees and agents, assets, information and systems. It also outlines the basis for the information/data security measures to be taken in the individual business areas of the Metropolitan Council.

The overall intention of this policy and its corresponding standards is to achieve and maintain an effective and appropriate level of information security within the Metropolitan Council and to reinforce the position of the Metropolitan Council as a trusted agency.

All employees and agents of the Council must be aware of their responsibility with regard to the issue of security and be proactive in exercising this responsibility. The Metropolitan Council Information Security Policy defines the security objectives, while the objective to the Metropolitan Council Information Security Standards is to provide authorized users with instructions that enable them to abide by the security requirements.

III. Background and reasons for policy:

The Metropolitan Council recognizes that appropriate information security measures are required to support business processes and protect information assets at the Metropolitan

Council. Information and assets are at risk from potential threats that range from employee error to malicious or criminal action, system failure and natural disasters.

The Metropolitan Council is committed to protecting its employees, assets, information and systems from misuse. An important aspect of information security is the assurance that only authorized users have access to Metropolitan Council information resources, and that the use of those resources is conducted in a professional manner, consistent with Council policy.

IV. Implementation/Accountability:

Implementation of this policy will be Council-wide, with the Information Services Department providing strategic planning and implementation assistance for designated projects. It is important that all Metropolitan Council, its staff and agents recognize their role within the Council and what potential security issues they face. Information systems users are required to comply with this policy and observe the related security standards. External parties are obliged to comply with the security standards in the course of their work at the Metropolitan Council.