Information Technology (IT) Policy

DRAFT for Board approval on April 11, 2007

Statement of Policy:

Chicago Metropolitan Agency for Planning (CMAP) acquires, manages and maintains Information Technology (IT) resources to carry out its work program.

The term IT resources refers to CMAP's entire computer network. This policy includes, but is not limited to guidelines and standards for the use of all CMAP-managed computer hardware, computer software, internet use, and electronic data.

This policy applies to all users of CMAP IT resources. Users of CMAP IT resources include all employees, contractors, consultants, temporary workers, or other authorized persons.

Utilizing CMAP IT resources by any means constitutes agreement with and consent to enforcement of this policy.

Statement of Purpose:

The purpose of this policy is to provide users with organizational guidelines and standards for appropriate usage of IT resources.

Statement of Procedure:

1. Employees are provided with access to IT resources to assist them in meeting their accountabilities to CMAP.

2. An account permitting access to CMAP IT resources may be provided to non-employees for purposes of conducting specific CMAP-related work only and will be deactivated upon completion of the agreed upon work.

3. Users are not entitled to any expectation of personal privacy in anything they create, store, send or receive using CMAP IT resources.

4. CMAP reserves the right to access, audit, block, delete, disclose, intercept, monitor, publish, recover, restrict, restore, review, screen or trace any information on the CMAP computer system at any time without notice.

5. If it is determined that an employee has used IT resources in violation of this policy, the employee will be subject to appropriate disciplinary action for misuse of CMAP property, up to and including discharge.

Computer hardware

1. All users are provided with access to the computer hardware needed to carry out their CMAP accountabilities. At a minimum, this includes a desktop workstation.

2. Access to selected network peripherals such as color printers, plotters, projectors and selected data servers may be restricted based on demonstrated need.

Portable electronic hardware

1. Portable IT computer hardware includes any CMAP-owned electronic equipment that can be easily disconnected and carried by an individual. Examples of portable computer hardware include: laptop computers, digital cameras, and wireless communication devices.

2. Portable computer hardware is issued to users only at the discretion of the Executive Director in consultation with appropriate Deputies.

3. Users of portable computer-hardware are responsible for taking reasonable precautions to safeguard it from theft or damage. Failure to do so may result in disciplinary action and restricted access to CMAP IT resources.

4. Portable computer hardware, when on CMAP premises, are required to be physically in the user's presence, locked to a user's desktop, or stored in a locked cabinet or office.

Computer software

1. All users are provided with access to the computer software needed to carry out their CMAP accountabilities. At a minimum, this includes a single designated standard suite of desktop productivity software including e-mail application, internet browser, word processing, spreadsheet and database management.

2. Users are expected to utilize this standard suite of desktop productivity software for all CMAP applications.

3. Installation of any software on CMAP-owned equipment is to be conducted only by an authorized IT resource administrator.

4. Installation of non-standard desktop productivity software on CMAP-owned equipment is not permitted.

Internet

1. All workstations are equipped with an internet connection providing access to the World Wide Web. Internet access is provided to facilitate work-related business and communications.

2. CMAP's network is protected by an internet "firewall" intended to shield IT resources from malicious viruses, programs or other electronic menaces. User's are prohibited from taking any actions to bypass this firewall or otherwise compromise the security of CMAP IT resources.

3. Use of the Internet in any way that may be disruptive or offensive to others is prohibited. Examples of inappropriate use of the Internet include: visiting sites or downloading material that contains sexually explicit or obscene information, ethnic or racial slurs or any other transmission that may be perceived as harassment or disparagement of other individuals based on their sex, race, sexual orientation, age, national origin or religious or political beliefs.

4. Users should be alert to the danger of receiving or transmitting data and executable programs via the Internet. Any file downloaded from the Internet should be checked for viruses using CMAP supplied anti-virus software.

5. Downloading files for entertainment, personal business, or any purpose unrelated to CMAP business is not permitted.

Electronic Data

1. CMAP IT resources include extensive holdings of electronic data. Many of these holdings are critical to the mission and data-to-day operation of CMAP. Users are expected to handle electronic data with utmost care and consideration.

2. All users are expected to take reasonable steps to safeguard all CMAP electronic information from being electronically corrupted or lost.

3. Users should be aware that most CMAP electronic datasets are subject to disclosure under the Freedom of Information Act. Precautions are taken to safeguard individual privacy with regard to personnel matters by restricting access to some administrative and executive file locations to appropriate personnel.

4. Any electronic data stored on any CMAP owned device is the property of CMAP. All information created, stored or transmitted from the CMAP network should be related to CMAP business. Material specifically prohibited from the CMAP network includes fraudulent, sexually explicit, profane, obscene, defamatory images or statements. Also prohibited are images or statements intended to harass, embarrass or intimidate.

5. CMAP IT resources may not be used for the creation, storage, production or dissemination of commercial or personal advertisements, solicitations or promotions.

6. CMAP IT resources may not be used for the creation, storage, production or dissemination of destructive computer programs (e.g. viruses, worms, Trojan horses).

7. CMAP IT resources may not be used for the creation, storage, production or dissemination of material that is political or religious in nature.