PROCUREMENT POLICY & PROCEDURE DIRECTIVE

SUBJECT: INFORMATION TECHNOLOGY SECURITY POLICY

ORIGINATING OFFICE: **Information Technology Division**

1. **PURPOSE**: The purpose of this policy directive is to establish and implement an information technology security policy for the Office of Contracting and Procurement.

2. **AUTHORITY**: This policy directive is being promulgated pursuant to:

   a) Section 202 of the District of Columbia Procurement Practices Act of 1985 (1985), effective February 21, 1986 (D.C. Law 6-85; D.C. Official Code §2-301.01), as amended by sections 101 and 105 of the Procurement Reform Amendment Act of 1996, effective April 9, 1997 (D.C. Law 11-259; D.C. Official Code §2-302.02);

   b) The District of Columbia Administrative Procedures Act of 1975 (DC APA), effective October 8, 1975, (D.C. Law 1-19; D.C. Official Code §2-501 et seq.);

   c) The District of Columbia Freedom of Information Act (DC FOIA), effective March 25, 1977 (D.C. Law 1-96; D.C. Official Code §2-531 et seq.); and

   d) The United States Copyright Act of 1976 (USCA) (P.L. 94-553, 90 Stat. 2541) (Oct. 19, 1976) (17 U.S.C. §§1-8, 10-12, and 107).

3. **APPLICABILITY**: This policy directive shall apply to Office of Contracting and Procurement (OCP) employees, contractors, consultants, and volunteers, herein referred to as "users," who utilize OCP's information technology (IT) equipment and computer system.

4. POLICY AND PROCEDURE STATEMENT:

4.1 Protection of OCP Information.

4.1.1 All users are expected to abide by OCP IT policies, procedures and guidelines.

4.1.2 Unless otherwise specified, the computers maintained by OCP for business purposes are the property of OCP.

4.1.3 OCP IT equipment includes, but is not limited to, computer software and hardware (i.e., printers, scanners, workstations, laptop computers, digital cameras, and modems).

4.1.4 A user is responsible for protecting confidential OCP-related information and documents from unauthorized access, modification, duplication, destruction, or disclosure.

4.1.5 Information stored on OCP computers in an electronic format shall be considered a "public record" under §2-502(18) of the DC APA and, as such, shall be treated as either confidential or disclosable to the same extent as other government documents and records.

4.2 The Right to Privacy and Electronic Communications.

4.2.1 Electronic communication capabilities shall be provided to users in order to facilitate communication and to satisfy OCP's business needs and purposes.

4.2.2 "Electronic communications" include, but are not limited to, electronic mail (e-mails) and their attachments, facsimiles, and telephonic or voice-mail messages.

4.2.3 Since most electronic communications create a record that can be archived and retrieved, and because OCP stores its network activity on a daily basis, electronic communications are the property of OCP.

4.2.4 Users have no expectation of privacy in anything created, stored, sent or received on OCP's electronic communication system.

4.2.5 Sending or attempting to send abusive, defamatory, discriminatory, disruptive, harassing, obscene, offensive, or threatening information, statements or

electronic communications of any kind, to another user from an OCP computer, is prohibited.

4.2.6 Incidental personal use of OCP's electronic communication system shall be permitted, but such use:

(a) Shall not violate any federal or D.C. government laws or regulations, or OCP policies, procedures and guidelines; and

(b) Shall be restricted to non-work hours.

4.3 Copyright and Software License Compliance.

4.3.1 It shall be the policy of OCP to respect computer software copyrights, and to adhere to the terms of software licenses to which OCP is a party.

4.3.2 Unless expressly authorized to do so by written agreement with a license owner or author, a user is prohibited from duplicating any licensed software or related documentation (except for backup and archival purposes) for use either on OCP's premises or elsewhere.

4.3.3 Unauthorized use or duplication of software may subject a user to civil or criminal penalties under the USCA, including fines or imprisonment.

4.4 Use of the Internet.

4.4.1 For purposes of this policy directive, all information retrieved from the Internet:

(a) Shall be considered copyrighted; and

(b) If retrieved for government work-related purposes, shall be a permitted, fair use under the USCA.

4.4.2 Copying, sending or receiving trademarked, copyrighted, proprietary information, or other materials such as documents, graphics, video clips, audio clips, or third-party software, without the express written permission of the copyright owner or the proper license, is prohibited.

4.4.3 During work hours, OCP computers, its network and the Internet shall only be used for OCP business needs and purposes.

4.4.4 All Internet usage, including downloading information, is monitored by the District of Columbia Office of the Chief Technology Officer, and is subject to review by OCP management without notification to the individual user.

4.4.5 The transmission of sensitive OCP-related information (such as information concerning employees, claims, client lists, purchase cards, and vendors, or the unauthorized transfers of software) by a user via the Internet shall be prohibited, except that the names, salaries, titles, and dates of employment of all District employees are considered to be public information which shall remain available to the public.

4.4.6 If OCP management determines that a user has abused his or her Internet privilege, the individual's ability to access the Internet from an OCP computer may be modified or terminated, and the appropriate disciplinary action may be taken.

4.4.7 A user is prohibited from using OCP computers to access, display, store, or transmit pornographic materials or other information of a political, sexually explicit, racially offensive, or religious nature.

4.5 Acquisition and Installation of Hardware and Software.

4.5.1 All acquired hardware and software used on OCP computer systems shall be obtained by using established procurement procedures, including purchase orders, purchase cards, petty cash, lease or rental agreements, and trial use.

4.5.2 A user shall not attach non-OCP owned computer hardware to any OCP IT equipment or asset.

4.5.3 OCP reserves the right to inventory and inspect all hardware and software on each OCP-owned computer or laptop.

4.6 Virus Detection.

4.6.1 A "computer virus" is defined as any computer software program that causes or influences either hardware or software to operate in a manner contrary to the intentions of, or in a manner not approved by, the original owner or user of the software or hardware.

4.6.2 Computer viruses may be intentionally or inadvertently introduced directly into a computer in order to spread to or be replicated in other systems through the use of diskettes or CD-ROMs, or may be acquired from external sources such

as by opening an e-mail from an unknown author or downloading files from Internet sites.

4.6.3 It is each user's responsibility to:

(a) Use reasonable care to prevent the introduction of viruses into OCP's computer system;

(b) Immediately contact the OCP Help Desk (724-4735) if assistance is needed to clean or purge an infected file or diskette; and

(c) Scan any incoming business-related or personal e-mail messages with attachments prior to opening by using OCP's virus protection software, and delete (without forwarding) such e-mails if a virus is detected.

4.7 Mobile Computer Usage.

4.7.1 The policies and procedures established by OCP pursuant to this policy directive shall also apply to OCP computer resources used outside the office.

4.7.2 A user shall exercise reasonable precautions to protect OCP computers from theft or unauthorized access.

4.7.3 Only approved hardware and software shall be used to remotely connect OCP computers to the DCWAN, the District government-owned computer network shared by multiple agencies.

4.7.4 OCP computer hardware and software provided for remote access purposes shall not be altered or enhanced.

4.7.5 A user shall return OCP computer hardware to OCP once the user either terminates his or her OCP employment or relationship, or is transferred to a different agency.

4.7.6 Remote computer access shall be permitted for users, and shall be limited to a specific business need or purpose.

4.8 Computer Security.

4.8.1 A user:

(a) Is responsible for respecting the privacy of others;

(b) Shall not monitor, access, read, alter, or copy another user's computer file without first obtaining proper authorization;

(c) Shall not access or attempt to access without authority a restricted computer area or file pertaining to an OCP computer system, including by-passing OCP's data protection measures or uncovering security loopholes;

(d) Shall not alter any OCP-installed software protections or restrictions placed on OCP computer applications, files or directories;

(e) Shall turn off his or her OCP desktop computer prior to leaving the office at the end of the workday in order to prevent security breeches involving the desktop hard drive and the OCP network; and

(f) Shall use password-protected screen savers to prevent security breeches while away from their computer.

4.9 OCP-Issued Computer Identification and Passwords.

4.9.1 A user shall be responsible for:

(a) Safeguarding passwords used to access OCP's computer system; and

(b) All activity generated from an OCP-issued identification and password.

4.9.2 A user shall not:

(a) Send e-mails under a name or address other than his or her own, officially-designated District government e-mail address; or

(b) Add, remove or modify identifying network header information in an effort to deceive or mislead e-mail recipients.

4.9.3 A terminated user's supervisor shall promptly notify the OCP Help Desk (724-4735) of the termination so that the user's computer identification and password can be disabled.

4.10 General Use of OCP Computer Resources.

4.10.1 A user shall be permitted access to the OCP computer system in order to perform his or her job.

4.10.2 Personal use of the OCP computer system by a user is a privilege that may be revoked by OCP management at any time.

4.10.3 A user shall use OCP computer resources in a professional, ethical and lawful manner.

4.10.4 The use of OCP's computer system and network in order to gain unauthorized access to remote computer systems shall be prohibited.

4.10.5 A user shall not waste computer resources by sending mass mailings or chain letters; subscribing to non-business-related servers and mailing lists; spending excessive amounts of time on the Internet; playing games; or otherwise creating unnecessary or inappropriate network traffic.

4.10.6 A user shall not electronically transmit audio and video files except for business-related purposes since the transmissions require significant network resources.

4.11 Disciplinary Action.

4.11.1 A user who violates this policy directive may be subject to corrective action, which may include reprimand, termination or suspension, and may be held personally liable for any claims or damages.

5. **APPENDICES**: None.

6. **AMENDS OR SUPERSEDES**: This policy directive supercedes OCPD 1803.00 effective March 13, 2002.

7. **EFFECTIVE DATE**: This policy directive shall become effective on July 17, 2003.

8. **EXPIRATION DATE**: This policy directive shall expire on July 17, 2005.

_____ _____

Jacques Abadie III, CPCM **Date**
Director, Office of Contracting and Procurement
District of Columbia Chief Procurement Officer