
 MUNICIPALITY OF ANCHORAGE O P E R A T I N G P O L I C Y / P R O C E D U R E	P&P No. 28-9	Page 1 of 10
	Effective Date: August 27, 2019	
Subject: Business Use and Access Control	Supercedes No. 16-3	Dated:
	Approved by: 	

1. PURPOSE

To define the appropriate use of MOA information systems, assets, and resources for authorized users. This policy defines the business use and acceptable personal use of MOA devices with the MOA's networks (Wide-area-networks (WAN) or local-area networks (LAN) for employees and contractors.

The objectives of this policy are to:

- a. Reduce security risks
- b. Protect the integrity of MOA systems and data
- c. Comply with regulatory requirements

2. POLICY

It is the policy of the Municipality to establish and maintain Municipal-wide Business Use and Access Control of all MOA owned computer systems and/or networked devices.

3. ORGANIZATIONS AFFECTED

All Municipal agencies.

4. REFERENCES

NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST SP 800-53 Access Control, MOA Policy 40-16 against harassment, PP 28-7 Password Management, 17 USC 107 Copyrights.

5. DEFINITIONS

(1) **Access Control**

The principle of limiting access to information assets only to appropriate individuals. See also: *Information Assets*.

(2) **Administrative Account**

A specific category of account on an information system characterized by heightened privilege. See also: *Information System*.

- (3) **Authentication**
The process of validating a user's claimed identity using one or more authentication factors. See also: *Identity Management, Authentication Factors*.
- (4) **Botnet**
A specific category of malware characterized by remote control of numerous information systems for illicit (and often illegal) purposes. See also: *Malware*.
- (5) **Denial of Service**
A cyber-attack in which the perpetrator seeks to make a machine or network resources unavailable to its intended users by disrupting services.
- (6) **Encryption**
A technical security control used to protect the confidentiality of an information asset. See also: *Information Asset, Confidentiality, Technical Security Control*.
- (7) **Executive Management**
Senior or top-level management, with statutory authority to make business, financial, and operational decisions and changes within an MOA department, corporation or commission. These are generally exempt positions that hold the liability for department functions, service programs or other activity of department staff.
- (8) **File Transfer Protocol (FTP) Site**
A site used to transfer files between a client and a server or a computer network.
- (9) **Information Asset**
Information owned, held in trust, stewarded or otherwise maintained by the MOA for any purpose. See also: *Information System, Information Owner*.
- (10) **Information System**
A discrete set of information resources organized for the collection processing, maintenance, use, sharing, dissemination, or disposition of information.
- (11) **Local Area Network (LAN)**
A communications network connecting various hardware devices together within a building by means of a continuous cable or an in-house voice-data telephone system.
- (12) **Malicious Software**
Software designed to circumvent one or more security controls and/or create damage that would compromise security
- (13) **Malware**
Software designed to interfere with a computer's normal function. See also: *Malicious Software*.
- (14) **Network Sniffer**
A software utility or a device used to passively eavesdrop, collect or analyze information packets on a network.
- (15) **Password Cracker**
A software utility or a device used for the purpose of obtaining passwords – usually via brute force. See also: *Authentication*.

- (16) **Peer-to-Peer Network**
A distributed data sharing network often times used to share copyrighted music, software, and movies.
- (17) **Ping Flood**
A simple denial-of-service attack where the attacker overwhelms the victim with ICMP "echo requests" packets.
- (18) **Prohibited**
To forbid, by authority, access to any established list, objective or action; such as in reference to forbidden sites – e.g. pornographic, gambling, etc.
- (19) **Proxy Server**
A computer within the networks system that acts as an intermediary for requests from users seeking resources from other servers. A user connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. If the request is validated by the filter, the proxy server provides the resource by connecting to the relevant server and requesting the service on behalf of the user.
- (20) **Remote Access**
The ability to get access to a computer or a network from a remote distance.
- (21) **Trojan Horse**
A specific category of malware disguised as a useful computer program that contains concealed instructions which, when activated, performs an illicit or malicious action (e.g. as destroying data files). See also: *Malware*.
- (22) **Usenet**
A worldwide distributed discussion or communication system available on computers.
- (23) **Virtual Private Network (VPN)**
A technical security control designed to ensure confidentiality, integrity, and availability of information transmitted between two points across a public network. See also: *Confidentiality, Integrity, and Availability*.
- (24) **Virus**
A specific malware category of a computer program that is usually hidden within another seemingly innocuous program which produces copies of itself and inserts them into other programs and usually performs a malicious action such as destroying data. See also: *Malware*.
- (25) **Vulnerability Scanner**
A software package or device used for the purpose of enumerating software vulnerabilities on a given host. See also: *Software Vulnerability*.
- (26) **WAN**
Wide Area Network.

6. RESPONSIBILITIES

- a. The Chief Information Security Officer (CISO) shall be responsible for oversight of all MOA Information security.
- b. Records owned by the Departments are subject to oversight as designated by Executive Management under AMC 3.95.

7. PROCEDURE

a. Access for Authorized Purposes

- (1) Personnel must use MOA networks and associated systems for authorized purposes only, related to MOA business and their job duties except as authorized in subsection 7.j., "Personal use of MOA equipment".
- (2) Personnel must not access MOA information, programs, or systems when such access is not required for an authorized business purpose. This includes system administrators who must have system access right due to their job responsibilities.
- (3) No Administrator may view or otherwise access a MOA user's information without the express consent of the user, Executive Management or the Department of Employee Relations.

b. Personal Computing Equipment Prohibited Use

- (1) Employees must not connect personal computing equipment (laptops, PC, workstations, servers, cellular devices or other networking equipment) within the internal MOA WAN or LAN other than the exceptions set forth in b.(2)
- (2) Cellular or computing equipment approved for stipends are allowed to access MOA associated systems for business use within the guidelines of MOA Policies.

c. Contractors Computing Equipment Authorization

- (1) Contractors may use their personal or company owned devices within the MOA WAN or LAN for authorized purposes only, related to MOA business and their job duties.

These devices are subject to all Municipal policies when connecting to the MOA networks and will be monitored, reported and audited for security purposes.

d. Application of Passwords

- (1) Authorized users to manage passwords in accordance with P&P 28-7.

e. Use of Issued Credentials

- (1) Personnel must use only the user IDs, network addresses, and network connections authorized by the MOA or Office of Information Technology staff to access MOA networks and associated systems.

f. Unauthorized Security Credentials

- (1) Personnel must not download, install, or execute any security program or utility (e.g. password cracker, network sniffer, vulnerability scanner) designed to reveal weaknesses in the security of a system without explicit authorization from the CISO. The MOA system is regularly scanned and violation of policy will be immediately acted on.

g. Execution of Electronic Information

- (1) Employees must not open files from unrecognized sources without confirming authenticity of message and sender.
- (2) When in doubt contact sender through alternate communication method (phone call) to verify message and attachment or call MOA IT helpdesk for additional guidance when opening files that have been sent to, or received by, them either electronically or on removable media, i.e. CD/DVD, USB Flash drive.
 - a. Examples of such files are email attachments received from unknown senders, files downloaded from the Internet or non-MOA FTP sites.
 - b. Any and all of these items can contain viruses, e-mail bombs, Trojan-horse code, spyware/ad-ware, BOT net, other malware, or inappropriate material and should be suspected.

- c. If contractors with MOA business suspect any of the above listed items they should notify their client supervisor immediately for remediation in all efforts to protect the MOA.

h. Unacceptable Use

- (1) Under no circumstances are personnel of the MOA authorized to engage in any activity using MOA technology or devices that is illegal under municipal, state, or federal law.
- (2) Prohibited email and communication activities and prohibited system and network activities are listed below and will be strictly enforced.
 - a. Personnel may be exempted from some of these restrictions during the course of their valid job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services or the requirement of a law enforcement investigation); however, cautious and meticulous adherence must be followed by all users.
 - b. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
 - c. Any form of harassment via email, instant messaging, telephone, paging, or other electronic means, whether through language, frequency, or size of messages.
 - d. Unauthorized use or forging of email header information.
 - e. Solicitation of email for any other email address, other than that of the poster's account, with the intent of harass or to collect replies.
 - f. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
 - g. Use of unsolicited email originating from within MOA networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by MOA or connected via the MOA's network.
 - h. Posting the same or similar non-business-related messages to large numbers of Usenet news groups or web forums.

- i. Use for access to or distribution of indecent or obscene material, or child pornography.
- j. Use for commercial activities, including advertising, unless specific to charter, mission, or duties of the government agency.
- k. Use for political activities, partisan activities, lobbying or outside business.
- l. Use of MOA Information technology resources for personal gain.

i. System and Network Prohibited Activities

- (1) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the MOA.
- (2) Unauthorized copying of Copyright Material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the MOA or the end user does not have an active license unless such copying constitutes fair use of a copyrighted work pursuant to 17 USC 107.
- (3) Exporting software, technical information, encryption software or technology, in violation of federal export control laws. The appropriate management should be consulted prior to export of any material that is in question.
- (4) Introduction of malicious programs into MOA information technology resources (e.g., introducing viruses, worms, Trojan horses, e-mail bombs, etc. into the MOA network or individual MOA computing devices).
- (5) Revealing account information to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- (6) Using MOA computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws including MOA Policy 40-16 against harassment.
- (7) Making unauthorized offers of products, items, or services originating from any MOA account.

- (8) Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forging route information for malicious purposes.
- (9) Network vulnerability testing, security scanning, virus or trojan horse testing or executing any form of network monitoring, which will intercept data not intended for the employee's host.
- (10) Any activity, application or service that circumvents security solutions, services, controls, user authentication, security of any host, network or account, or interfering with or denying service to any authorized user or service is prohibited and strictly enforced. (e.g., URL filtering, network monitoring, remote access requirements through MOA virtual private network, MOA ingress/egress access control requirements, McAfee, and other security solution, service, or control, intentionally creating a denial of service to a user, applications, host, network, or other MOA process.)
- (11) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, another user's terminal session, via any means, locally or via the Internet/intranet/extranet.
- (12) Providing information about, or lists of, MOA employees to any outside parties, except as authorized.
- (13) Any personal use of private or confidential information of any individual obtained by an employee as a result of performance of job duties or as a result of their employment with the Municipality of Anchorage.
- (14) Use of encryption (at rest or in transit) without an approved business case justification and written approval from the Incident Response Team (IRT) and the CISO.
- (15) Uses of peer-to-peer (P2P) file transfer solutions without an approved business case justification and written approval from the IRT and the CISO.
- (16) Use of unauthorized remote-control technologies.
- (17) Use of non-operating system standard screen saver or other similar technologies.
- (18) Use of any external proxy systems or other similar technologies.
- (19) Turning off or tampering with security solutions.

j. Personal Use of MOA Issued Equipment

- (1) Under the Municipal Ethics Code, Municipal employees may not divert or permit the diversion of Municipal issued equipment for a purpose unrelated to municipal business. This policy establishes that for, MOA owned computing equipment and systems (cellular devices), in the course of normal business, incidental personal use is acceptable only under the following guidelines:
 - a. Cell phones, Smartphones, Laptop computers and Tablets when used for voice calls or data – Personal use that does not exceed the greater of 30 minutes or 5% of the minutes allowance under the applicable services plan is presumed insignificant, but any personal use that results in increased cost must be reimbursed to the Municipality in full. (In the case of unlimited use plans, personal use may not exceed the greater of 30 minutes or 5% of total use.)
 - b. Desktop computers, Laptop computers, Smartphones, and Tablets when used on non-cellular land or wireless based networks that do not require pay by use plans – Personal use is presumed insignificant so long as it does not occur during scheduled work hours and there are no additional costs attributable to personal use.
- (2) The employee is required to reimburse the Municipality for all overages that are incurred outside of the approved data plan.
- (3) If improper personal use of Municipal equipment is identified, the supervisor may conduct an investigation with guidance from Employee Relations and the employee may be subject to discipline. Serious violations include recurring misuse after direction to stop or misuse resulting in substantial personal benefit may warrant serious discipline up to and including termination.

k. Least Privilege

- (1) Personnel tasked with a network administrative account must ensure that network and system access controls are configured to limit the privileges extended to users to the least necessary to accomplish authorized business purposes.

8. ANNUAL REVIEW DATE/LEAD REVIEW AGENCY

Subject:	Business Use and Access Control	P&P No. 28-9	Page 10 of 10
----------	--	-----------------	----------------------

The Office of Information Technology will review this document in October of each year for any needed revisions.