Document Type:	Regulation
Number:	4.30d
Effective:	10-01-07
Revised:	01-01-11
Legal References:	

PDA AND MASS STORAGE DEVICE REGULATION

I. INTRODUCTION

The purpose of this regulation is to provide employees with guidance governing auxiliary devices that may connect to the City's network and computers and to provide conditions for business use of these devices. The goals of this regulation are to provide increased utility and access for City employees, to control support costs, and to achieve responsible information stewardship.

Personal Digital Assistants (PDA's) and other electronic devices provide high-availability access to email and schedules and ease the transference of information, while becoming a growing challenge to support given their increasing functionality, capacity, prevalence combined with increasing numbers of vendors, models and service options. Because of their ability to introduce information into and take information away from the City's infrastructure, they also pose a security concern.

This regulation governs the introduction, use, and support of PDAs and mass storage devices by employees of the City of Boise, and others who have a business relationship with the City.

II. SCOPE

For the purposes of this regulation, personal digital assistants (PDAs) are defined as devices providing one or more of the following functions:

A. A handheld computing device running productivity applications tools for personal information management
B. Synchronization of the device with desktop software applications
C. Wireless communications with information services (e.g. email) while attached to the City's network

PDA devices vary in capability and form and include, but are not limited to, some mobile phones, communicators, Pocket PCs, Palm OS devices, Blackberries and other mobile devices. For the purposes of this regulation, mass storage devices are defined as devices providing one or more of the following functions:

A. Devices that provide digital storage capacity used for storing, transferring and carrying data
B. Synchronization of the device with desktop software applications or the desktop operating system
C. Wired or wireless communications with information services (e.g. the Internet) while attached to the City's network

Mass storage devices vary in capability and form and include such devices as flash memory storage devices (also known as USB Keys, Jump Drives, Thumb Drives, Flash Drives and Pen Drives), Zip drives, MP3 Players, iPods, and so forth.

Devices that connect to the City's PCs must be able to operate under "User" level security. Those that require "Administrator" access to operate are not allowed.

Boise City Information & Technology Department and its team members are charged with managing the City's computing infrastructure and this regulation. City Supervisors and Managers are charged with determining the suitability of purchasing and introducing these devices into the City, given the expected utility, cost, and security threat of use of these devices.

III. REQUIRED APPROVAL

Manager/supervisor approval is required to purchase a Personal Digital Assistant (PDA) or Mass Storage Device or any other device that can connect to the City's network or computers and download, upload, or store data.

Only City approved PDA or Mass Storage Devices may be used on the City's infrastructure. The Information & Technology Department maintains a list of allowed and supported devices. An exception to this general rule is made when an outside entity provides information on a device for temporary, immediate use by the City. In this case, the device must be surrendered to City personnel, who then can read from the device on City equipment outfitted with a current virus scanner. For example, a presentation loaded on a non-employee's USB Memory Device for use within the City.

IV. SECURITY

The devices covered by this regulation are not considered secure computing devices.

A. Only non-confidential information should be stored on these devices
B. If a password protection feature is offered, it must be enabled
C. If encryption is provided on the device, it must be enabled
D. Passwords should never be stored on these devices unless they are encrypted
E. When not in use, they must be secured in a locked cabinet or drawer to prevent loss or theft

V. MONITORING AND PRIVACY

The City monitors the use of its PDA's and mass storage devices to ensure that these resources are used effectively, appropriately, legally, and in accordance with the City's policies and regulations. The City may monitor randomly, in response to a particular problem, or, in some cases, continuously. The City reserves the right to inspect any and all information stored on or in PDA's and mass storage devices. The City also reserves the right to inspect any and all messages and data sent and received. The City may also choose or be required to publicize this data.

Employees using the City's PDA's and mass storage devices expressly waive any right of privacy in anything they create, store, send, or receive on a City PDA or mass storage device or through the City provided Internet, other computer network and/or any other City resources.

Employees should not consider any electronic communication, media or services to be either private or secure. Although PDA's and mass storage devices can be protected by passwords, employees should not assume that the passwords provide them with

privacy or ownership of the PDA or mass storage device account or the records within them.

VI. MISCELLANEOUS

Implementing and supporting traditional computer desktop-centric PDAs tends to be very labor-intensive activities that challenge the overall return on investment of personal productivity devices. Wireless server-based synchronization can meet the requirements of personal information management with less time involved in the support required for desktop-based devices, and the information is likely to be more up-to-date.