Procedural Directive

California State University
Northridge
Department of Police Services

To:	All Department of Police Services Personnel
Subject:	Responsible Use of University Computing Resources
Directive Number:	2007-08
Date:	December 18, 2019
Amends/Supersedes:	October 24, 2007 version; February 16, 2011 version; January 7, 2015 version.
Approved:	Gregory L. Murphy, Chief of Police

I. Objective:

In keeping with the University's policy on the Use of Computing Resources, this document outlines requirements and guidelines for the use of computing systems and facilities used or operated by the Department of Police Services and located at California State University, Northridge or operated by California State University, Northridge (CSUN) employees. This includes, but is not limited to, any computer, server, or network provided or supported by CSUN. The purpose of this directive is to ensure that all employees and partners use the CSUN computing facilities in an effective, efficient, ethical, and lawful manner.

II. Procedures:

A. Appropriate and Responsible Use

Central to appropriate and responsible use is the stipulation that, in general, computing resources are provided for the completion of academic requirements, scholarship, and University business. Personal (non-commercial) use is permitted as long as such use is incidental – that is, occasional – and does not place a burdensome load on resources and does not interfere with any employee assignments, tasks or duties and responsibilities. An example of acceptable personal use would be to check a personal email account a few times a day. Conversely, an example of inappropriate personal use would be searching the internet for a car for a couple of hours. All uses inconsistent with these objectives are considered to be inappropriate use and may jeopardize further access to services and result in disciplinary action.

B. User Responsibilities

In the text below "Users" refers to CSUN employees and contractor's using CSUN/DPS computing systems and facilities. Within the department this includes all staff and student employees or volunteers.

To respect the privacy of others:

1. Users shall not attempt to access any data or programs contained on the CSUN system that they do not have authorization for or the consent of the owner of the data or program.
2. Users shall not divulge sensitive personal data to which they have access concerning faculty, staff, or students without explicit authorization to do so.
3. Users are responsible for protecting any information used and/or stored on their desktop.

To respect the intended usage of resources:

4. Users shall not share their computer or CSUN account passwords with anyone.
5. Users are not to make copies of copyrighted materials, except where permitted by law or by the owner of the copyright. This includes, but is not limited to, software, electronic documents, video files, and audio files.
6. User shall not make copies of system configuration files (e.g. etc/password or the SAM file) for their own, unauthorized personal use or to provide to other people or users for unauthorized use.
7. Users shall not use campus computing resources for any personal commercial venture.

To respect the shared nature of resources:

8. Users shall not purposefully engage in activity with the intent to harass other users; degrade the performance of systems; prevent authorized CSUN employees use of CSUN resource; obtain extra resources beyond those allocated; circumvent CSUN computer-security measures; violate any local, state or federal law; or gain access to CSUN systems for which proper authorization has not been given.
9. Users shall not consume excessive network bandwidth by downloading files such as MP3 or Real Audio or by using streaming audio or video unless required as part of their job responsibilities.

To respect the integrity of system and network resources:

10. Users are requested to immediately report any weakness in computing security or any incidents of possible misuse or violation of this agreement to the CSUN Information Security Officer via their respective department manager.
11. Users shall not download, install, or run security programs or utilities that reveal weakness in the security of a systems. For example, CSUN users shall not run password-cracking programs on CSUN computing systems.
12. Certain positions require the ability to run security analysis programs on network and systems. The following positions have management authorization to run programs necessary to perform these tasks at CSUN:

    Information Security Officer
    Security Analyst
    System Administrator
    Network Analyst

C. Department of Police Services Hardware and Software Requirements

Only software authorized by the Chief of Police may be operated on Department of Police Services computing systems. A list of the current authorized software is attached to this procedural directive. Periodically this list will be revised and maintained and accessible from the DPS IT Lead. Any specialized software which an employee wishes to utilize for a business purpose which is not included on this list will be required to have the written authorization from the Chief of Police prior to installation and use of the software. All requests for software authorizations from the Chief of Police shall be referred through the chain of command (for civilian and student staff through their immediate supervisor).

Under no circumstances shall any employee install personal software on a business computer or download any programs/software to a business computer for personal use or any use not authorized for the course and conduct of the individual's work responsibilities. The only exception to this requirement shall be for screensaver software. Employees may choose their own appropriate screensavers which are suitable and professional for the business environment. However, employees are to consult with the department's IT staff prior to installation of any screensavers to ensure software is compatible with department systems and that the screensaver will not in any way interfere with business applications.

The Chief of Police, in consultation with the Special Services Captain and department IT staff (and designated staff of campus IT and Administration and Finance Division) shall determine the computing brands and hardware to be utilized by employees within the department. No employee may replace, enhance, add to or otherwise install any hardware or workstation which has not been authorized by the Chief of Police or her/his designee.

D. University Policies and Procedures

All employees are accountable and responsible for adhering to university policies and procedures concerning or relating to the use of computing resources. Those policies may be accessed via the campus IT website or the Administration and Finance university policy and procedure website.

DPS Authorized Software List - as of December 2019
Alertus Desktop (*Pushed out from Server - Central IT*)
Microsoft Forefront Endpoint Protection (*Pushed out from server- Central IT*)
Microsoft .NET Framework
SCCM {System Center Configuration Manager} (*Pushed out from server- Central IT*)
Flexera (*Pushed out from server - Central IT*)
Adobe Shockwave Player
Adobe Flash Player
QuickTime Player
Google Chrome
Microsoft Internet Explorer
Mozilla Firefox
Java Runtime Environment (32-bit only)
Malwarebytes
Microsoft Office Professional Plus 2019 (x86) - Access
Microsoft Office Professional Plus 2019 (x86) - Excel
Microsoft Office Professional Plus 2019 (x86) - InfoPath
Microsoft Office Professional Plus 2019 (x86) - OneNote
Microsoft Office Professional Plus 2019 (x86) - Outlook
Microsoft Office Professional Plus 2019 (x86) - PowerPoint
Microsoft Office Professional Plus 2019 (x86) - Publisher
Microsoft Office Professional Plus 2019 (x86) - Skype
Microsoft Office Professional Plus 2019 (x86) - Word
Microsoft Office Professional 2013 - 2016 (x86)
Microsoft Visio
CCleaner
Printer Drivers (*Department Document Center Printers & Standalone*)
Spybot – Search & Destroy
7-zip
Roxio Creator
Dell CyberLink Power DVD
Dell Support Assist
Microsoft SQL Server & Client Software
Microsoft Server
Linux Server & Desktop Software
Oracle VM VirtualBox
Microsoft Windows 7
Microsoft Windows 10
RIMS - CAD

RIMS - Reports
RIMS - Maps
RIMS - 911 to Test
RIMS - E911
RIMS - Property Room
RIMS - Mobile
RIMS - Officer Field Reporting
ArcGIS - Mapping & GIS Software
AudioLog Client Software
JDIC
DMV Pull Notice Software
SIS - Alarm Center
TMS - Training Software
Indenti-Kit
Intellex Player
Text to 911 Client
CopWare Software
CANUTEC's ERGO 2016
AXON - BodyCam Evidence Sync & Taser Software
CCTV - CaseCracker - Interview Room Management System
CCURE Server & Client Software
CCTV - HDVR Server & Client
Campus CCTV - IBM Intelligent Video Analytics Software
Campus CCTV - Milestone xProtect Smart Client Software
OmniLock Software
Motorola - Radio Programming Software
Motorola - Radio Dispatching Software
Adobe Reader
Adobe Creative Cloud License
Adobe Acrobat DC 2018 - Creative Cloud
Adobe Animate and Mobile Device Packaging 2018 - Creative Cloud
Adobe Audition 2018 – Creative Cloud
Adobe Bridge 2018 – Creative Cloud
Adobe Camera Raw 2018 – Creative Cloud
Adobe Character Animator 2018 - Creative Cloud
Adobe Creative Cloud License
Adobe Dreamweaver 2018 - Creative Cloud
Adobe Illustrator 2018 – Creative Cloud
Adobe InCopy 2018 – Creative Cloud

Adobe Lightroom Classic 2018 – Creative Cloud
Adobe Media Encoder 2018
Adobe Premier Pro 2018 - Creative Cloud
Adobe Preview 2018 – Creative Cloud
Adobe After Effects 2018 - Creative Cloud
Adobe Photoshop 2018 - Creative Cloud
Adobe InDesign 2018 - Creative Cloud
Techsmith Snagit 2018
FileZilla 3.25.1
CSUN Fonts
Microsoft Teams
Microsoft Power BI Desktop (x64)
Camtasia 2019
EquatIO
Read&Write 12
Citrix Workspace 1909
Zoom 4.5.2
Airtame
Cintrix Receiver 4.9.7 LTR CU7
Box Drive 2.7
GlobalProtect 5.0.1-9
Google Earth Pro
Apple iTunes 12.9
Google Chrome Ver. 72.0.3626.121
Snagit 2019
OrgPublisher PluginX 11.4
Onbase Unity Client 18
Box Desktop
Box Sync
Avery Design Software
VPN - Pulse Secure
VLC Software
SSH Secure Shell
Photo Camera Software
Video camera Software
Label Maker Software
UPS Software
AutoCAD AutoDesk Software
TurboCAD
Recuva

VZAccess Manager
GreenWorx Lighting Control Client
Retunity+
SecurityDesk LPR client
Parallels (*Mac Only*)
Pages (*Mac Only*)
Numbers (*Mac Only*)
KeyNote (*Mac Only*)