



Arkansas Department of Community Correction

Two Union National Plaza Building
105 West Capitol, 2nd Floor
Little Rock, Arkansas 72201-5731
(501) 682-9510 Fax: (501) 682-9513

ADMINISTRATIVE DIRECTIVE: 09-07

COMPUTER AND CELL PHONE RESOURCES

TO: DEPARTMENT OF COMMUNITY CORRECTION EMPLOYEES

FROM: G. DAVID GUNTARP, DIRECTOR

SUPERSEDES: AD 08-04

PAGE 1

APPROVED: Signature on File

EFFECTIVE DATE: May 29, 2009

- I. APPLICABILITY.** This policy applies to Department of Community Correction (DCC) employees, contractors, volunteers, extra help, offenders, and others authorized by the Director to use DCC computer resources.
- II. POLICY.** Computer resources are to be used only for official State business.
- III. DEFINITIONS.**
- A. Computer.** Any desktop, laptop, workstation, server, handheld, palm-top, smart-phone, or other electronic device capable of accessing and using any state domain or network resource.
 - B. DCC Domain.** DCC.ARKGOV.NET is the agency domain for access to DCC computer resources and systems managed by the IT staff.
 - C. Hard drive/hard disk** – common data storage device within a computer that stores various information (operating systems, applications, folders, and files) on internal magnetic disks or platters.
 - D. ITA.** Information Technology Administrator.
 - E. ITS.** Information Technology Section.
 - F. Mission Critical Data.** Any DCC work related information that more than one DCC employee must retain or access to fulfill their official duties.

- G. Network.** Computers, printers, scanners, audio/visual display devices, or telephones interconnected by telecommunication equipment, cables, or wireless technology used to transmit or receive information within the DCC domain.
- H. Permissions.** The varying levels of rights to access specific network computers, equipment, systems, servers, folders, files, or databases as granted to various users by the ITA.
- I. Server.** Specifically configured computers used to make applications, databases, websites, and files available to computers throughout the network.
- J. System.** The working combination of hardware, software, and data communications devices used to perform DCC duties.
- K. User.** Any person authorized to access the DCC network.

IV. COMPUTER GUIDELINES.

A. Purpose for Computer Resources

1. DCC provides computers and systems to ensure effective access to and use of State resources to perform DCC duties. A systematic method is used for computer hardware and software acquisition, operation, security, maintenance and/or upgrades, technical support, access control and repair to optimize DCC and State resources. (4-ACRS-7D-05[P])
2. The ITA manages the DCC Information Technology Plan for maintaining computer resources consistent with budget approvals and in accordance with the Arkansas Information Systems Act 914 of 1997.

B. Privacy/Confidentiality

1. All DCC provided computers, servers, software, email accounts and messages and information stored in the same are State-property. There is no expectation of privacy related to the information entered, received, or transmitted on these systems. Management has the authority and capability to monitor, track, and record any and all activities involving DCC systems. Monitoring is not done to intimidate or harass, rather it is to ensure proper use of computer resources. DCC users will cooperate with management and Internal Affairs regarding any audit requests. Internal Affairs will conduct random audits of computer resources to ensure compliance with this policy.
2. Users who have access to privileged or sensitive information shall not disclose that information to any source except to those authorized by the DCC Director and for no other purpose than conducting approved DCC business. (2-CO-1F-06, 3-3111)

C. Security.

1. General. The ITA or designee reserves the right to review and adapt any and all security measures related to DCC computer systems to ensure the security of all information which these systems transmit or store.
2. User Accounts. The ITA or designee will assign user identifications (IDs). The user ID will be made available only for the period of employment with DCC or as otherwise authorized by the Director. The ITA is authorized to suspend or deactivate user accounts being used for unauthorized purposes.
3. Passwords.
 - a. Users are assigned an initial password to log into the DCC network, but are required to change it to a secret password known only to the user. Users are required to change passwords every 90 days. Passwords must be at least nine characters in length and include at least three of the following four character types: upper case (A-Z), lower case (a-z), special characters (!@#\$%^&*()), and numerals (0-9).
 - b. The combination of user ID and password uniquely identifies each user within the DCC/State network. Users must keep passwords private and must not divulge their password to any other person. Users must immediately notify ITS if they have reason to believe their password has been compromised.
4. Physical Security. Supervisors and any assigned property custodian must ensure computers are in a secure location as office layout permits. Computer displays should face away from windows and doors to minimize the possibility of information being viewed by unauthorized persons. Doors to offices containing computers are to be locked when the user is absent for an extended period of time. Users may request electronic security services such as proximity or biometric devices for those computers used around offenders (e.g., in kitchen areas of the Centers) to prevent possible access by unauthorized persons. All DCC computers are configured to automatically enter a password-protected screen saver mode after 10 minutes of inactivity.
5. Electronic Security.
 - a. Users are to be aware, and notify ITS of any attempts to compromise DCC systems or information by unauthorized parties.
 - b. DCC employees *shall not* store or transport any confidential information on any external storage media or devices, such as floppy disks, CD-ROMS, DVD-ROMS, external hard drives, flash memory including thumb-drives and memory cards, without prior written approval of the Director.

6. Supervisor's Security Responsibilities.
 - a. Monitor user's computer use and take action to resolve situations of abuse. When considered appropriate, contact the next person in the supervisory chain to analyze.
 - b. Require service/repair personnel to be properly identified and ensure the presence of a DCC employee while repairs are being made.
 - c. Immediately notify ITS when user's employment is terminated.
7. Offender Rules Pertaining to Computer Resources. Offenders are prohibited from using any DCC computer that is connected to the State network or the Internet.

D. Backup and Recovery.

1. Server data will be backed up on a regular basis to an external media to facilitate secure off-site storage. Backups will cover reasonable recent use periods as well as archival timeframes.
2. Recovery tests are conducted with every backup job.

E. Computer Resource Use and Rules. Computer resources are to be used only for official State business. Upon entering the assigned user ID and password, users automatically agree to accept responsibility for and compliance with this policy and to use DCC computers appropriately.

1. Users must not
 - a. connect a personally owned computer to the DCC network without written authorization from the ITA and the Chief Deputy Director.
 - b. use, submit, publish, display, or transmit information to or from a DCC computer which violates or infringes on the rights of another person, is defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory or illegal, or any other content which could in any way, shape, or form offend another person or cause public embarrassment to the DCC.
 - c. restrict or inhibit other DCC users from using DCC computer resources.
 - d. use or attempt to use unauthorized computer resources, monitoring tools, network programs/testers, packet sniffing, remote access, key stroke recognition technology, or remote control equipment and software.

- e. misuse DCC email accounts. DCC email accounts are not to be used for such correspondence as personal memberships, accounts, newsletters, advertising, auctions, or others that may result in a return of spam-type email traffic.
 - f. use the system for any illegal purpose, or for personal gain.
 - g. use or initiate processes that degrade the efficiency of the computer system(s) such as unofficial chat rooms, channel subscriptions, or receipt of streaming or broadcast audio or video via the Internet.
 - h. mask or otherwise falsify the user's identity.
 - i. modify computer configurations, installed programs or system facilities.
 - j. compromise or attempt to compromise the integrity of any computer system.
 - k. establish unauthorized network services including web pages, servers, FTP servers, and Telnet services.
 - l. move or delete files that do not pertain to your assigned work.
 - m. download or share audio (music), mp3, games, computer software or video files that could expose DCC to legal claims based on copyright infringement or other legal challenges.
 - n. Use DCC computer resources inappropriately.
 - o. send such mail as chain letters, virus hoaxes, urban legends.
2. Users must
- a. comply with information disclosure policies. Files and electronic messages may be accessible under the Freedom of Information Act.
 - b. comply with the Department's Record Management policy. Information contained or transmitted via the DCC systems, including e-mail, is subject to the Arkansas Records Retention Act. It is the responsibility of each user to understand which records must be maintained. Refer to policy regarding Records Management for further information.
 - c. ensure data entry into DCC electronic systems is accurate. Supervisors are responsible to periodically check for data accuracy through routine verification techniques and ensure systems that have staff input (e.g., intranet team sites) contain appropriate material. Policies pertaining to specific computer systems may provide further requirements for data verification. (3-3111[P]).

- d. store mission critical data in appropriate Departmental folders to ensure availability for appropriate personnel. Permissions and access to Departmental folders is granted to respective departmental members only. Contact ITS for any questions regarding folder structure and permissions setup.
- e. store work-related but “personal data” (i.e., prefilled out leave or time records) within a users’ server based personal folders. Mission Critical data can only be stored on the space on a server drive for temporary periods or work-in-progress situations. Personal folders’ size is limited. All are viewable only to their owners, however they are randomly scanned by ITS periodically for inappropriate material
- f. immediately notify the supervisory chain of any evidence of child pornography on any computer system and await further instructions. ***DO NOT TOUCH THE COMPUTER ANY FURTHER NOR TURN IT OFF.***
- g. immediately notify supervisors if inappropriate web pages are accidentally viewed. Failure to properly notify management will be considered intentional viewing by the user.
- h. notify the supervisor of any abnormal or suspect activities seen on computer resources and the supervisor will contact the ITA.

F. Installing Software. Software is pre-installed on computers and configured by the ITS. To comply with copyright laws and ensure compatibility with the DCC and the State networks, only authorized software may be installed. Users must obtain written permission from the ITA before installing any software on DCC computer resources. Unless specifically authorized, employees may not install, download or access any software or programs such as chat rooms or instant messengers, peer-to-peer file-sharing, screensavers, antivirus, spyware or malware tools, toolbars, hard drive or system imaging or ghosting. Users must not change any of the ITS system configuration default settings.

G. Technical Support.

1. ITS will provide primary technical support for all DCC systems. Users are encouraged to attempt to resolve issues themselves using any appropriate support information provided.
2. Users must not allow persons outside the agency to use or attempt to fix computers unless approved by the ITA or designee to provide support.

H. Planning for Computer Resources. DCC provides the use of computers and electronic services to ensure effective use of State resources. A systematic method is used for computer hardware and software acquisition, operation, security, maintenance and/or upgrades, technical support, access control and repair to optimize DCC and State resources. (4-ACRS-7D-05[P])

I. Ordering Computer Resources & Services. Computer purchase requests require written justification and the approval of the Chief Deputy Director to ensure compatibility and consistency with the Information Technology Plan. Refer to the Administrative Services policy, "Purchasing" section for guidance on purchasing computer resources. The Director is the authority for acquiring all fee-based online services, e.g., electronic subscriptions. Prior to processing such requests, the ITA must be in receipt of a requisition authorized by the Director.

J. Outside Agency Systems. The Chief Deputy Director, Deputy Director or Assistant Director will authorize access to specific protected outside agency databases (e.g., e-OMIS, ACIC/NCIC) as appropriate and deemed necessary for employees to perform their job functions. Activity involving those data bases shall be governed by the rules and regulations imposed by the agency providing access.

K. New Technology. Due to the ever changing nature of electronics and computer systems, new technology will inevitably arise that may not be fully covered within this policy. Any and all new technology not covered must be evaluated and authorized by the ITA prior to usage on the DCC network.

L. Penalties for Violations. Violations of this policy will be dealt with in accordance with the Employee Code of Ethics and Rules of Conduct and the Employee Discipline policies.

M. Quantity of Employees with Internet Access. Of the DCC employees, approximately 70% will be assigned personal computers. Approximately 78% of all the DCC employees will have continual access to Internet services through personal work stations or common access stations.

V. CELL PHONE/COMMUNICATION DEVICE GUIDELINES. Agency issued cell phones and other communication devices are for state business use only. No employee is authorized to download games, ring-tones, ring-back tones or any other personalized, non-business related feature of the device. Any employee that downloads non-business features shall reimburse the agency for the expense and maybe subject to disciplinary action.

A. Employees with communication devices are responsible for the following:

1. Securing and maintaining the device.
2. Immediately reporting any missing and/or stolen device.

3. Adhering to any building restrictions on use or possession of the device while on that property. Under no circumstances are DCC employee's allowed to carry a non-state issued cell phone or other communication device into a DCC or ADC residential facility.
4. Limiting outgoing text messages to State business and not to exceed 300 per month.
5. Notifying the supervisor when authorized out-of-state travel will likely cause roaming charges.