APB

Public service with fairness and integrity

Arkansas Parole Board

Two Union Plaza Building
105 West Capitol Ste. 500
Little Rock, AR 72201-5731
Phone: 501-682-3850
Fax: 501-682-5351
www.paroleboard.arkansas.gov

EXECUTIVE SUMMARY

SUBJECT: 18-02 TECHNOLOGY RESOURCES USE

SUPERSEDES: 08-01 Computer Resource Use &
08-02 Cell Phone Use

APPLICABILITY: This policy applies to APB Members, Staff, and other authorized by the Chairman, or designee, to use APB computer resources and/or wireless cellular devices.

APPROVED: Chairman John Felts **EFFECTIVE DATE:** 05/19/18

POLICY: It is APB policy to allow use of computers and electronic services, as appropriate, and to ensure that State resources are effectively utilized. A systematic method will be used for computer hardware and software acquisition, operation, security, maintenance/upgrade, technical support, control, and repair to optimize computer resources. Computing resources are provided by the APB to enhance communication, share information, increase efficiency, and perform the administrative duties of the APB and further the mission.

EXPLANATION: This policy provides a framework for the maintenance, security, and use of technology resources. It combines two previously implemented directives and is reflective of changes in position titles along with technological advances and the manner and frequency of use of technology resources.

Arkansas Parole Board
Two Union National Plaza Building
105 West Capitol; 5th Floor
Little Rock, AR 72201-5731
(501) 682-3850 Fax: (501) 683-5381

ADMINISTRATIVE DIRECTIVE: ~~08-01~~18-02 ~~COMPUTER~~ TECHNOLOGY RESOURCES USE

TO: ARKANSAS PAROLE BOARD

FROM: ~~LEROY BROWNLEE~~JOHN FELTS, ~~CHARIMAN~~ CHAIRMAN
~~PAGE 1 of 7~~

SUPERSEDES: 08-01 Computer Resource Use ~~AD 06-02 (Signed May 3, 2006)~~
08-02 Cell Phone Use

APPROVED: SIGNATURE ON FILE EFFECTIVE DATE: ~~April 15, 2008~~May 19, 2018

I. APPLICABILITY. This ~~policy~~ directive applies to Arkansas Parole Board (APB) ~~Commissioners, Hearing Examiners, support staff, contractors, volunteers, extra help,~~members, staff, ~~offenders,~~ and others authorized by the Chairman, or designee, to use APB computers and/or wireless cellular devices. Violators of this directive may be subject to disciplinary action to include termination.

II. POLICY. It is APB policy to ~~provide~~ allow use of computers and electronic services, as appropriate, and to ensure effective ~~use of~~ that State resources. A systematic method will be used for computer hardware and software acquisition, operation, security, maintenance/upgrade, technical support, control, and repair to optimize computer resources. Computing resources are provided by the APB to enhance communication, share information, increase efficiency, and perform the administrative duties of the APB and further ~~the~~ its mission. Many of the computers and electronic services are shared with the Department of Community Correction (~~DCC~~ACC) and the Department of Correction (ADC). They allow access to the ~~INTERNET~~Internet, electronic mail and bulletin boards, internal and external databases, library catalogs, work-related professional organizations, etc. Computers and electronic services are provided for the performance of official State business and the enhancement of ~~the skills and knowledge necessary for such~~employee skills/training necessary for maximum performance. Personal use of APB computers, wireless/cellular devices, and all electronic services is strictly prohibited. Cell phones/communication devices will be distributed to designated staff members upon approval of the Chairman, or designee. Distributing cell phones/communication devices to appropriate staff members is meant to enhance the efficiency and effectiveness of APB operations.

III. DEFINITIONS.

A. Computer Resources. Computers and computer related equipment, servers, local and wide area networks and input and output devices.

B. Software. Applications and programs installed on computers.

C. Computer Security. Aspects associated with providing availability, integrity, and confidentiality of information on APB computers.

D. Electronic Services. Services include, but are not limited to, access to the ~~DCC~~ ACC and State networks, eOMIS, Internet access, electronic mail (E~~-Mail~~mail) and other online services.

E. Offenders. Offenders are probationers, parolees, community correction center residents, and ADC inmates.

F. Permissions. System settings that grant, deny, or limit access to various computer systems, file folders, programs, and documents.

G. User. Persons authorized access to APB computer resources.

IV. ~~PENALTIES.~~ ~~Violators (Hearing Examiners and support staff) of this policy are subject to penalties ranging from verbal warnings to employment termination. Commissioners who violate this policy will be reported to the Governor's Office, by the Chairman, for appropriate action.~~**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 non-business related applications, ringtones, ring-back tones or other personalized, non-business related features to the device. Any employee that downloads non-business related features shall reimburse the agency for any expense and will be subject to disciplinary action, up to and including termination.

A. Employees with cell phones/communication devices are responsible for:

1. Securing and maintaining any issued cell phone or other communication device.
2. Immediately reporting any missing and/or stolen device to his/her immediate supervisor, or the appropriate IT and/or HR/Fiscal personnel.
3. Adhering to any building restrictions on use or possession of a cell phone/communication device while on that property. Under no circumstances are APB employees allowed to carry a non-state issued cell phone or communication device into an ACC residential center or ADC facility.

B. The Board's Systems Coordination Analyst is responsible for:

1. On a monthly basis auditing the usage of all APB cell phones/communication devices and reporting all suspected abuses to the Executive Administrator.

V. COMPUTER GUIDELINES.

A. Technical Support. ~~Employees/Hearing Examiners/Commissioners~~All members and staff should ~~always~~ use the appropriate help options and manuals provided with the computer system prior to asking for assistance. When an employee cannot resolve system or software problems, ~~they~~ he/she should contact the ~~User Support~~ Systems Coordination Analyst for further assistance.

Users must not allow ~~people~~ individuals from outside of the agency to use or attempt to fix computers unless the person ~~is~~ has been approved by the ~~User Support~~Systems Coordination Analyst to provide support ~~or the person is known to be working as an authorized contractor or Department of Information Services (DIS) employee.~~ .

B. Planning for Computer Resources. ~~APB 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 APB and State resources. The ~~User Support~~Systems Coordination Analyst maintains the APB Information Technology Plan for maintaining computer resources consistent with budget approvals and in accordance with ~~the Arkansas Information Systems Act 914 of 1997.~~applicable State law, rules, and regulations.

C. Ordering Computer Resources & Services. Computer and related hardware purchase requests require a written justification to the Executive Administrator and the approval of the Chairman to ensure compatibility and consistency with the Information Technology Plan.

D. Installing Software. Software is pre-installed on computers and configured by the ~~User Support~~ Systems Coordination Analyst. In order to guarantee compliance with copyright laws and insure compatibility with the ~~DCC~~ ACC and the State networks, only authorized software may be installed. Users must obtain ~~permission~~ written authorization from the ~~User Support Analyst~~ Systems Coordination Analyst before installing any software on APB computer resources. Users must not change any of the established defaults for security and/or computer access.

E. Security Measures.

1. **User Accounts.** The ~~DCC~~ Systems Coordination Analyst or an ACC designee will assign user identifications (IDs). The user ID will be made available only for the period of employment with APB or as otherwise authorized by the Executive Administrator or Chairman. ~~The~~ An authorized employee of ~~DCC~~ ACC or the APB ~~User Support~~Systems Coordination Analyst ~~is authorized to~~may suspend or deactivate user accounts being used for unauthorized purposes. Notice of any suspension or deactivation shall be provided to the employee's immediate supervisor, the Executive Administrator, and the Chairman.

2. **Passwords.** Users are assigned an initial password to log into the ~~DCC~~ACC/State network, but are required to change it to a secret password known only to them. Users ~~are~~ will be periodically required to change passwords ~~every 90 days~~. ~~Previously used passwords may not be reused until five password changes have occurred. Passwords must be at least nine characters in length and include at least three of the following four character types: UPPER CASE, lower case, special character and number.~~All passwords generated for accessing the APB Wi-Fi network should be safeguarded and may not be shared with anyone absent permission of the Systems Coordination Analyst. For assistance in constructing easily remembered passwords, contact the ~~User Support~~Systems Coordination Analyst.

   The combination of user ID and password uniquely identifies each user within the ~~DCC~~ACC/State network. Users must keep passwords private and must not divulge their password to any other person, including their supervisor. Users must immediately notify the ~~User Support~~Systems Coordination Analyst if they have reason to believe their password has been compromised. ~~APB computers are configured to automatically enter a password-protected screen saver mode after 10 minutes of inactivity.~~

3. **Physical Security.** Supervisors and ~~any assigned property custodian~~the Board's Business Operations Manager must ensure computers are in ~~a~~ the most 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.

4. **E~~e~~-Mail Security/Privacy.** The use of the state electronic mail (~~e-Mail~~email) is neither private nor secure. APB management has the right to access any ~~e-Mail~~ email communication of any APB employee without ~~their~~ his/her consent and/or knowledge.

F. Supervisor's Security Responsibilities.

Monitor employee's computer resource use and take action to resolve situations of abuse.

G. Fiscal/HR Section Responsibilities.

~~b. Require service/repair personnel to be properly identified and ensure the presence of an APB employee while repairs are being made.~~

1. Immediately notify the ~~User Support~~Systems Coordination Analyst when a supervised employee is terminated.
2. Take action to resolve suspected abuse. When considered appropriate, contact the next person in the supervisory chain to analyze.

H. ~~User Support~~Systems Coordination Analyst Responsibilities.

1. ~~Notify the DCC IT Administrator of any viruses and other unusual activity on the computer system.~~Require service/repair personnel to be properly identified and ensure the presence of an APB employee while repairs are being made.
2. Notify the ACC IT Administrator or designee of any viruses and/or other unusual activity on the computer system.
3. Notify the ~~DCC~~ ACC IT Administrator or designee when an employee ends their employment with the agency and ~~insure~~ ensure ~~their~~ his/her account is closed.
4. Immediately notify the ~~DCC~~ ACC IT Administrator or designee when the APB suspends any account because of misuse.
5. Conduct periodic ~~supervisory~~ reviews of computer and systems access permissions and notify the ~~DCC~~ ACC IT Administrator when the APB makes any changes.

~~F~~I. Privacy, Monitoring and Audits. Since all computers and software are APB-owned, all information stored on the computer is the property of the APB. There is no level of privacy related to the information entered, received, or transmitted. ~~Management~~ The Agency has the authority and capability to monitor, track, and record any and all transactions made on your computer. Monitoring is not done to intimidate or harass, rather it is to ensure proper use of computer resources. The ~~User Support~~Systems Coordination Analyst will conduct random audits of computing resources to ensure compliance with this policy.

~~G~~J. Data/File Management.

1. **Electronic Mail (~~e-Mail~~Email).** Email~~e-Mail~~ messages may be subject to the State's Record Retention policy which establishes mandatory retention periods of ~~state~~ certain documents. All employees must comply with the Record Retention policy when reviewing and retaining ~~e-Mail~~email communications. All retained files and electronic messages may be accessible under Freedom of Information Act (FOIA).

2. **Data Folders & Filing Documents.** 'Mission critical' data must be stored in appropriate folders located on the networked drive designated by the ~~DCC~~ ACC Information Technology Section to ensure availability for all personnel who are authorized to access the folder. Data on this location is backed up and can be restored in the event of a hardware failure, whereas data stored on a local computer hard drive are not backed up and would be lost. Contact the ~~User Support~~APB Systems Coordination Analyst for any questions regarding folder structure and permissions setup.

   Data not intended for sharing should be stored on the networked drive designated by the ~~DCC~~ ACC Information Technology Section for personal (work-related) use. This

drive is viewable only to the owners and the ~~DCC~~ ACC/APB Information Technology Sections but is subject to random review.

3. **Data Verification.** Employees are responsible for entering accurate data into eOMIS and other computer systems. Supervisors must periodically check for data accuracy through routine~~, systematic~~ verification techniques and take necessary steps to counsel/discipline employees who repeatedly enter inaccurate data. Policy for specific computer systems may provide further requirements for data.

~~H~~K. **External Database Access.** The Chairman is the sole authority for granting access to specific protected outside agency databases as appropriate and deemed necessary for an employee to perform job functions (i.e., eOMIS, ACIC/NCIC, VINE~~S~~, AASIS, etc). Activity involving ~~those~~ these databases shall be governed by the rules and regulations imposed by the agency providing access.

~~I.~~L. **Website Changes.** Only the ~~User Support~~ Systems Coordination Analyst, when authorized by the Chairman or designee, may make authorized changes to APB website.

~~J~~M. **Offender Rules Pertaining to Computer Resources.** Offenders are prohibited from using any APB computer, service, or wireless/cellular device. ~~that is connected to the State network or the Internet.~~ They are also prohibited from using any standalone machine containing personnel, offender, or security information or any other agency records. ~~agency business, or security records.~~ Any employee who facilitates prohibited offender access shall be subject to immediate termination.

~~K.~~VI. **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 APB computers appropriately. Inappropriate or unacceptable use by users is the basis for disciplinary action. Although every situation that pertains to inappropriate use of APB computing resources and electronic services cannot be listed, the following is included to provide an understanding as to the type of conduct that is acceptable and unacceptable. The Chairman, or designee, reserves the right to approve or disapprove other activities ~~which compromise APB computer systems~~.

A. **Users <u>shall not:</u>**

~~a.~~ 1. Connect a personally owned computer or computer hardware to the state network.

~~b.~~ 2. Use, submit, publish, display, or transmit information which~~:,~~ is defamatory, false, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive~~,~~ or otherwise biased, discriminatory or illegal material, or material that violates or infringes on the rights of another person, or any other statements which could cause public embarrassment to the APB.

~~c.~~ 3. Restrict or inhibit other APB users from using APB computer resources.

~~d.~~4. 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.~~ 5. Use removable USB media (flash drives) or "thumb drives" without the Chairman or designee's written approval ~~of written justification~~. If approved for use, thumb drives must be encrypted and shall not be removed from the office without written permission from the Chairman.

~~f.~~ 6. Use the system for any illegal purpose~~,~~ or for personal gain.

~~g.~~ 7. Install or use "chat" or "instant messaging" software unless approved by the Chairman.

~~h.~~ 8. Use or initiate processes that degrade the efficiency of the computer system(s) such as memberships in chat rooms or receipt of streaming or broadcast audio or video via the Internet unless authorized by the ~~User Support Analyst~~Chairman or designee.

~~i.~~ 9. Mask or otherwise falsify a user's identity.

~~j.~~ 10. Modify computer configurations, installed programs, or system facilities.

~~k.~~ 11. Compromise or attempt to compromise the integrity of any computer system.

~~l.~~ 12. Establish unauthorized network services including web pages, servers, FTP servers, and Telnet services.

~~m.~~ 13. Move, alter, or delete files that do not pertain to your assigned work.

~~n.~~ 14. Download or share audio (music), mp3, games, computer software or video files that could expose APB to legal claims based on copyright infringement or other legal challenges.

~~o.~~15. Perform any other prohibited activity not specifically addressed ~~covered~~ by the inappropriate use statements included in this policy.

~~p. Send or forward any non work-related email messages via their state e-Mail account.~~

B. Users must:

~~a.~~ 1. Comply with written and verbal directives that address ~~information disclosure~~the use of technology resources.

~~b.~~2. Immediately notify management of any evidence of child pornography on any computer system. ~~In the event of finding, or suspecting, child pornography on any APB computer system *STOP AND DO NOT TOUCH THE COMPUTER ANY FURTHER*. Immediately notify the supervisory chain and await further instructions. Do not explore the computer any further for evidence or even turn it off.~~

~~c.~~ 3. Immediately notify his/her supervisor~~s~~ or another available supervisor if inappropriate web pages are accidentally viewed. Failure to properly notify ~~management~~ a supervisor will be considered intentional viewing by the user.

d. Notify ~~their~~ his/her supervisor of any abnormal or suspect activities seen on computer resources. The supervisor will contact the ~~User Support~~Systems Coordination Analyst as appropriate.

VII. ~~ATTACHMENTS~~FORMS

~~AD 08-01 Form 1 –~~Attachment 1: Employee Acknowledgement

Attachment 1

Employee Acknowledgement of Computer Resources Use Policy

Please acknowledge by signing that you have received, read, and ~~understood~~ understand the Arkansas Parole Board ~~Policy~~ Administrative Directive: ~~**Administrative Directive: 08-01 Computer Resources Use**~~
~~(*Supersedes Computer Resources Use AD 06-02*).~~

18-02 Technology Resources Use

It is your responsibility to read it thoroughly and ask questions of your supervisor if you don't understand it. All employees or officials of the Arkansas Parole Board are responsible for complying with all pertinent policies, directives, and memorandum. ~~The Fiscal Manager will place a signed copy of this form in your personnel file.~~

This form must be signed and returned to the ~~Fiscal~~ Business Operations Manager before an employee can use and APB computer resource, and a signed copy of this form will be placed in your personnel file.~~within five days after receipt of the above policy.~~

~~Employee Confirmation:~~

_____ _____ _____ _____

~~PRINT NAME~~ Employee Printed Name **Employee Signature** **~~DATE~~ Date**
~~SIGNATURE~~

~~Supervisor Confirmation:~~

_____ _____ _____ _____

~~PRINT NAME~~Supervisor Printed Name **Supervisor Signature**
~~DATE~~Date **~~SIGNATURE~~**

~~**NOTE:** This form must be signed and returned to the Fiscal Manger before an employee can use any APB computer resource.~~