State of Iowa Department of Corrections
Policy and Procedures

Policy Number: AD-PR-27
Applicability: Institutions, CBC, Central Office, IPI
Policy Code: Public Access
Iowa Code Reference: 716.6B
Chapter 1: Administration & Management
Sub Chapter: Personnel
Related IDOC Policies: AD-GA-19, AD-PR-11, AD-PR-29
Administrative Code Reference: NA
Subject: Utilization of Information Technology Resources
PREA Standards: NA
Responsibility: John Needleman
Effective Date: June 2023
Authority:

1. PURPOSE

To establish guidelines for the use of information technology resources in the Iowa Department of Corrections (IDOC), and to inform that these rules shall apply whenever a user accesses IDOC information technology resources.

2. POLICY

It is the policy of the IDOC to ensure its computer resources are used professionally and responsibly for purposes directly related to the operation of the state correctional system.

CONTENTS

3. DEFINITIONS – As used in this document:

A. Access – To instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network.

B. Computer – An electronic device that performs logical, arithmetical, and memory functions by manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, computer software, and communication facilities which are connected or related to the computer in a computer system or computer network.

C. Computer Network – A set of related, remotely connected devices and communication facilities including two or more computers with capability to transmit data among them through communication facilities.

D. Computer Program – An ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

E. Computer Software – A set of computer programs, procedures, or associated documentation used in the operation of a computer.

F. Computer System – Related, connected or unconnected, computers or peripheral equipment.

G. Data – A representation of information, knowledge, facts, concepts or instructions that have been prepared or are being prepared in a formalized manner and have been processed, or are intended to be processed in a computer. Data may be in any form including, but not limited to, printouts, storage media, and as stored in the memory of a computer.

H. Iowa Corrections Offender Network (ICON) – The computer system utilized by the State of Iowa to maintain data on all clients/incarcerated individuals supervised by IDOC.

I. Information Technology Resources – Those facilities, technologies and information resources required to accomplish information processing, storage and communication, whether individually controlled or shared, stand-alone or networked. Included in this definition are all electronic resources and computing and electronic communication devices and services, such as, but not limited to, computers, terminals, printers, modems, e-mail, Internet access, ICON database, multi-media, removable data storage devices, instructional materials, and any other computer and system peripherals.

J. Removable Media - such as, but not limited to, optical media, removable drives, USB thumb/flash drives, or memory cards.

K. Services – The use of a computer, computer system, or computer network and include, but are not limited to, computer time, data processing, and storage functions.

L. Social Networking Sites - Websites or services where people can contribute content and share information with others. This information typically includes photos, videos, text, news, blogs, profiles and current event information. As with all internet postings, once posted it cannot be permanently removed. Popular social networking sites include but are not limited to: Facebook, Twitter, YouTube, Flickr.

M. See IDOC Policy **AD-GA-16** for additional Definitions.

4. PROCEDURES

A. Workplace Monitoring

1. Employees have no reasonable expectation of privacy while using information technology resources of the IDOC as information technology resources are the property of the IDOC.

2. The IDOC reserves the right to review, copy, delete, or disclose information technology resources at any time.

3. The IDOC has the right to monitor any aspects of its computer operations, including employees, interns/volunteers, consultants, and contract personnel user accounts, files, e-mails, Internet sessions, and/or login sessions.

B. Permitted Uses

1. Information technology resources are to be used for:

    a. Communication and information exchange directly related to the mission, charter, or work of the IDOC.

    b. Advisory, standards, research, and analysis activities related to the user's work task and duties.

    c. Any other governmental administrative communications not requiring a high level of security.

2. Users must use computer resources in an ethical and lawful manner.

C. User Responsibilities

1. Passwords

a. Initial passwords are assigned by the site's Systems Administrator and they are the keys to security on the computer system.

b. Passwords must be treated as confidential information and the user is responsible for keeping his/her password secure.

c. Passwords are not to be shared with anyone, without permission from the IDOC Director, Warden/District Director, IDOC Chief Information Officer (CIO).

d. Users shall be held responsible if their passwords are shared and /or used by another person.

e. Password Rules

1) Passwords expire every 45 days.

2) Passwords must be at least eight characters long.

3) Passwords must contain three of these four characters (upper case, lower case, number, and punctuation).

4) The user log on ID cannot be part of the password.

5) The user account locks after five bad password attempts.

6) The last ten passwords are "remembered" and cannot be reused.

2. Workstation Security

To prevent potential breaches of security, users must log off the network or ensure the system is locked when away from their workstations. This may be accomplished by completely logging off the network or by locking the workstation to prevent another user from accessing it.

3. E-mail Use

a. IDOC e-mail accounts shall be used for job-related activities only.

1) Since IDOC makes this e-mail account available to users, all e-mails, received and sent, may be reviewed at any time by management.

2) Any inappropriate use of e-mail can be cause for discipline.

b. The security of e-mail to persons outside the IDOC must be considered less secure than transmissions or e-mails within the IDOC so confidentiality regarding clients/incarcerated individuals information must be considered. If it is necessary to send confidential information via email, the email must be secured and encrypted using the current IDOC encryption process.

c. Accessing e-mail during non-working hours is prohibited without prior written approval. Employees will not be compensated in any way for accessing email during non-working hours.

4. Internet Use

1. Internet access via IDOC shall be used for job-related activities.

2. All Internet use may be reviewed at any time by management.

3. Contacting an Internet site that would not be considered work related can be cause for discipline.

5. Electronic Files

a. Any files saved on the network or a user's local hard drive may be reviewed for content by management.

b. Anything considered not work related shall be removed.

c. Anything inappropriate shall be reviewed with the user and appropriate action taken.

d. Any electronic files or software applications, including but not limited to IDOC Web files, ICON, ICON Medical, CIR, ICON Banking, ICON Food, Kronos, Workday, Iowa Courts Online any source requiring credentials, etc. shall be treated as confidential, per IDOC Policy **AD-PR-29** *Confidentiality of Information*.

e. Access to files and/or software applications is determined by need and requires supervisory approval. It is the duty of the supervisor to determine what access will be granted.

f. Access to files and/or software applications shall be work related only and consistent with/related to the job duties performed by the person accessing the information. Employees shall not attempt to access information when not related to job duties without specific supervisory approval.

g. The creation and storage of IDOC information on any non-IDOC platform is prohibited without prior written approval.

D. Prohibited Uses

The rapidly changing nature of computer technology prevents the listing of all possible prohibited activities. If a particular activity is not expressly prohibited by this policy that does not mean that it is permitted. If in doubt, request clarification from your supervisor. The following list of computer technology resources utilized by employees of the IDOC is prohibited:

1. IDOC's e-mail and Internet shall not be used for:

   a. Composing, sending, displaying, printing, downloading, or forwarding material that is defamatory, false, inaccurate, abusive, embarrassing, obscene, pornographic, profane, sexually-oriented, political, religious (except as appropriate for job duties), threatening, intimidating, racially offensive, discriminatory, or illegal. Any employee encountering any of these types of material should report it to their supervisor immediately.

   b. Using e-mail for any commercial purposes for personal gain or profit, including personal messages offering to buy or sell goods or services.

   c. Sending or forwarding any item in violation of copyright law.

   d. Developing, sending, forwarding or responding to chain letters.

2. Computer software-licensing agreements, copyright, and publishing laws must not be violated. Software licensed/purchased by IDOC shall not be copied, distributed, or loaded for personal use.

3. Installing or playing electronic games is prohibited.

4. Personal online shopping is prohibited.

5. Gambling, wagering, betting, or selling chances is prohibited.

6. Intentionally seeking out information or obtaining copies of revealing, publicizing, or modifying files or other data that are private, confidential, proprietary, or not open to public inspection or release is not permitted unless specifically authorized to do so.

7. Users shall not intentionally enter or transmit computer viruses or any form of intentionally destructive programs. To protect against computer viruses and malware, individuals shall not bring in any software or removable media from outside unless specifically authorized by the IDOC Director, respective Deputy Director, Warden/District Director, or IDOC Chief Information Officer (CIO)/Designee. Selected employees may be authorized to access the system from their home via dial in, VPN, or e-mail as approved by the System Administrator. Use of personal computer equipment is prohibited without permission from Warden/District Director/Designee.

8. Software designed to destroy data, provide unauthorized access to computer systems, or disrupt computing processing in any way is prohibited.

9. Copying, modifying, replacing, or deleting any other user's account or any software used for system management is prohibited.

10. Employees shall not access or attempt to access computer programs and/or files for which they are not authorized, **Iowa Code 716.6B**.

11. Use of the internet to listen to audio or view video that is not work related is prohibited.

12. Use of the internet to access social networking sites is prohibited unless specifically authorized by the IDOC Director, respective Deputy Director, Warden/District Director, IDOC Chief Information Officer (CIO)/Designee or in compliance with IDOC Policy **AD-GA-19**, *IDOC Public Website Social Media Sites*.

13. Employees shall not engage in any activity that is intended to circumvent computer security controls by attempting to crack passwords, discover unprotected files, or to decode encrypted files.

14. Employees shall not alter or tamper with the computer, computer system, network, software, programs, data, documentation, or any other related property unless specifically authorized or requested to do so by the IDOC Director, respective Deputy Director, Warden/District Director, or IDOC Chief Information Officer (CIO)/Designee.

15. No client/incarcerated individual shall have access to any IDOC employee networked computer system unless specifically authorized by the IDOC Director, respective Deputy Director, Warden/District Director, or IDOC Chief Information Officer (CIO)/Designee. This prohibition does not apply to local area networks designed specifically for client/incarcerated individual use, nor does it apply to cloud based call center software employed by Iowa Prison Industries.

16. Employees shall not give information about the computer system, including software used by the IDOC, to anyone who is not an employee of the IDOC.

17. No outside agency or private vendor shall be granted access to the IDOC computer system without the express written permission of the IDOC Chief Information Officer (CIO)/Designee.

18. Employees shall not install any new or unapproved computer programs on any IDOC computers without the permission of the IDOC Chief Information Officer (CIO)/Designee.