State of Iowa Department of Corrections

Policy and Procedures

Policy Number: AD-IS-06
Applicability: Institutions, CBC, Central Office, IPI
Policy Code: Public Access
Iowa Code Reference: N/A
Chapter 3: ADMINISTRATION & MANAGEMENT
Sub Chapter: INFORMATION SYSTEM/RESEARCH
Related DOC Policies: AD-IS-07
Administrative Code Reference: N/A
Subject: CLIENT & INCARCERATED INDIVIDUAL OFFNET USAGE
PREA Standards: N/A
Responsibility: John Needelman
Effective Date: February 2024
Authority:

1. PURPOSE

To provide guidelines related to clients/incarcerated individuals' usage of information technology resources at Iowa Department of Corrections (IDOC) locations.

2. POLICY

It is the policy of the IDOC to ensure compliance of clients/incarcerated individuals' access to information technology resources within the state correctional system

CONTENTS

F. Print Services

G. User Responsibility

H. Data Sharing and Interconnection

3. DEFINITIONS

A. OffNet – Dedicated network(s) for use by clients/incarcerated individuals while housed at a correctional institution or residential facility.

B. Lab – A dedicated set of computers setup in a designated location designated for a defined function.

4. PROCEDURES

A. Centralized storage

1. Any clients/incarcerated individuals utilizing the OffNet shall be limited to 1GB of storage for all types of information stored. If individuals request additional storage, a long-term storage media solution may be allocated. Upon request a review shall be done by a committee designated by the IDOC Chief Information Officer (CIO) to authorize long term storage and set its constraints. If approved, a process will be created to allow access to long-term storage media based on a limited, pre-scheduled, and supervised basis. Said constraints shall be but are not limited to a reoccurring monetary fee

2. IDOC will keep files for six months after a client/incarcerated individual leaves an institution or residential facility.

3. IDOC will follow industry best practices to backup all OffNet systems and the data within. In the case of any or all systems catastrophic failure a best effort will be made to restore the environment in part or as a whole.

4. IDOC will put forth a best effort to restore deleted files two business days after receiving formal request to recover. This operation shall only be performed one time per 30-day period for any client/incarcerated individual.

B. Availability

Computer labs may be made available for use by incarcerated individuals or Clients. Security of said labs shall be consistent across all institutions and residential facilities supplying this resource.

C. Access

Passwords for OffNet access shall be generated and stored with authorization of IDOC CIO/Designee. New passwords may be generated by authorized staff within the central database. If new access rights are needed for immediate usage, the password will need to be set/reset manually on the OffNet by an authorized staff who also needs to make sure the afore mentioned central database reflects the change. Otherwise, at a minimum, a weekly automated process will generate new access permission with the updates also reflected in the afore mentioned central database.

D. Utilization

The OffNet shall only be utilized for select usage.

1. Authorized and properly sanctioned education opportunities
2. Personal documents
3. Legal documents
4. Authorized clerk work as part of a work assignment
5. Library services
6. Job search functions shall be restricted to authorized clients at residential facilities and incarcerated individuals in authorized Iowa Workforce Development (IWD) re-entry programs with OffNet resources available
7. Any form of programming, coding, scripting, or otherwise creating mechanisms to control information technology systems shall be restricted to those enrolled in authorized and sanctioned educational programs. The methods and tools used shall be those sanctioned by the IDOC CIO or designee as part of the curriculum. Written or electronic documents describing or instructing how to program, code, script, or otherwise create mechanisms to control information technology systems may be allowed.

The practice of said described techniques, if not explicitly connected to an authorized and sanctioned educational program, shall be prohibited. Usage not strictly within these bounds shall be a violation.

8. No general function OffNet information technology resource shall be used for Iowa Prison Industries (IPI) work.

E. Approved software

Only approved software shall be present on any information technology resource accessed by clients/incarcerated individuals. The software present shall be specific to the utilization that the specific client/incarcerated individual is authorized to utilize. Approved software for each of the authorized utilizations will be approved by the IDOC CIO/Designee.

F. Print Services

Print services can be made available at an institution or residential facility with OffNet resources that decides to offer them. In the case printing is allowed, the cost of this will be set at the site supplying the service.

G. User Responsibility

1. Passwords shall be treated as confidential information and the user shall be responsible for securing their password.

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

3. User accounts shall be locked out after five bad password attempts and can be unlocked by an authorized staff or will auto-unlock in an hour.

4. Access to the OffNet is a privilege and may be suspended or revoked at any time either by facility administration or the disciplinary process.

5. At the end of each session, the client/incarcerated individual shall log off/restart the session. Sessions shall not be shared.

6. Users shall not circumvent established security methods. Any attempt to do so may result in suspension/revocation of privilege.

7. Any and all forms of pornography (audio, video, graphics, and text) shall be prohibited on the OffNet. Any interaction with said materials may result in suspension/revocation of privilege.

8. Storage of audio and video files on the Offnet shall be prohibited; alternate listening or viewing means may be made available on a case-by-case basis.

9. There shall be no password protected or encrypted files owned, managed or created by clients/incarcerated individuals on the OffNet.

H. Data Sharing and Interconnection

1. Interconnections between staff and client/incarcerated individual systems shall be prohibited without the written authorization of the IDOC CIO/Designee.

2. General use devices on the OffNet shall have a wired connection.

3. Dedicated single-use devices (i.e. ADPS) available for any proctored testing/educational assessments may use a wireless connection

4. Clients/incarcerated individuals shall not be allowed to have administrative access to any information technology resource whether networked or isolated.

5. At Institutions, USB ports shall be disabled for all functionality outside of Human Interface Devices (HID) which have no internal storage.

6. Bluetooth radios shall be removed or hardware level disabled on all non-postsecondary education devices. For postsecondary education devices the usage of Bluetooth may be authorized by the IDOC CIO/Designee and shall be limited to HID devices only which have no internal storage.

7. Gaming systems and music devices shall have no network access while a client/incarcerated individual has access. When maintenance of these devices is being carried out by staff the devices shall not use the OffNet network or State network.

8. Access to resources outside the OffNet shall be restricted to those usages with advanced authorizations by the IDOC CIO.

    a. Educational outside access usage shall explicitly be handled by IDOC Policy **AD-IS-07**, *Incarcerated Individual Education Technologies*.

b. Clients at residential facilities and incarcerated individuals in authorized IWD re-entry programs may be allowed access to re-entry related search sites including but not limited to employment sites. Said sites shall be reviewed and authorized prior to clients at residential facilities and incarcerated individuals accessing them by IDOC CIO/Designee.