State of Indiana Indiana Department of Correction	Effective Date	Page 1 of	Number
	12/1/2020	4	04-05-103

POLICY AND ADMINISTRATIVE PROCEDURE
Manual of Policies and Procedures

Title
INFORMATION TECHNOLOGY SYSTEMS PASSWORD AND ACCOUNT SECURITY

Legal References (includes but is not limited to)	Related Policies/Procedures (includes but is not limited to)	Other References (includes but is not limited to)
11-8-5-2	04-03-101 04-03-103 04-03-111	IOT-CS-SEC-119

I. PURPOSE:

The purpose of this policy and administrative procedure is to establish Indiana Department of Correction (IDOC) computer user password security requirements to protect State information technology system assets.

II. POLICY STATEMENT:

It is the policy of the Indiana Department of Correction to protect its information technology (IT) system assets by establishing and managing security requirements for user passwords and personal user identifiers pursuant to the standards established by the Indiana Office of Technology (IOT). This policy and administrative procedure shall be reviewed annually and updated as necessary.

III. DEFINITIONS:

For the purpose of this policy and administrative procedure, the following definitions are presented:

A. ADMINISTRATIVE ACCOUNT: A privileged, higher level information technology system account that permits the account holder to grant system access, levels, rights, permissions and passwords to computer end users.

B. AUTHORIZED USER: An IDOC employee, contractor, intern, volunteer or other agent of the State who is authorized at a technical level to administer and support/maintain state computing information technology systems or is authorized at an end user level, to have access to and use State computing information technology systems and

telecommunications technology systems for business purposes on behalf of the State of Indiana.

C. PRIVILEGED USER ACCOUNTS: System asset user accounts, which have elevated access to make changes to system parameters and are assigned to authorized users at the technical level.

D. SYSTEM ASSETS: Computer hardware, telecommunications hardware and systems, digital devices such as digital copiers and facsimile machines, software, networks, the internet, IT information or data and/or IT services or IT resources that are made available by IDOC or IOT to authorized users and are necessary to conduct State government business and support the IT requirements of the IDOC and, therefore, must be protected by the appropriate security requirements to ensure business continuity.

IV. PROCEDURES:

A. Password Standards and Administration

1. User password protocols, including access levels, rights, and permissions for IDOC information technology systems shall be established pursuant to the standards established by the Executive Director of Technology.

2. The Executive Director of Technology Services shall designate staff responsible for managing administrative accounts that define password access levels, rights, and permissions for information technology systems used by IDOC employees or contractors.

B. Password and Logon Security

1. User passwords for information technology systems shall meet or exceed the following security standards as supported by the system:

   a. Minimum of eight (8) characters in length;
   b. Contain at least one (1) uppercase letter;
   c. Contain at least one (1) special character (e.g., !, @, #, $, etc.); and,
   d. Not contain personal user identifiers (e.g., SSN, DOB, phone number, etc.)

2. Smartphones are only required to have a four-digit password and are exempt from the complex password requirement.

3. IDOC information technology user accounts for all systems shall be associated with a single individual user and shall not be established for use for multiple users. The combination of a user identification and personal password shall authenticate a unique, individual employee or contractor user account. Exceptions must be approved by the Information Security Officer and the Executive Director of Technology Services.

4. Pursuant to the Information Resources Use Agreement (IRUA), all employees and contractors with access to IDOC information technology systems are prohibited from sharing their unique, individual usernames and passwords with anyone. In addition, all employees are prohibited from displaying their unique, individual usernames and passwords where others may view them.

5. IDOC users (employees and contractors) shall not, under any circumstance, use a "save password" option when using IDOC information technology systems to conduct State business.

6. Authorized users at the technical level that are assigned both user accounts and privileged user accounts shall not use the same password for multiple accounts. Instead, the authorized users shall maintain unique passwords for each account.

C. Account Deactivation

1. When an IDOC employee is terminated or is placed on administrative leave for any reason or when a contractor's service is terminated for any reason, all the employee's or contractor's information technology system accounts shall be immediately deactivated.

2. When an IDOC employee terminates service or a contractor terminates or otherwise closes a contract with the IDOC, all information technology system accounts assigned to the employee or contractor shall be deactivated.

3. When an IDOC employee or contractor transfers to another IDOC location or is reassigned to another position resulting in a change in job duties, the employee's supervisor, or in the case of a contractor, the appropriate management employee designated by the managing officer, shall assess the employee or contractor's access to IDOC information technology systems to determine if system access should be modified.

4. When an IDOC employee begins an extended leave of absence (FMLA, disability, military leave, etc.), all information technology system accounts assigned to the employee or contractor shall be deactivated or suspended.

XIV. APPLICABILITY:

This policy and administrative procedure is applicable to all Department facilities, staff, and offenders, except those offenders on Parole, and to those facilities that are operating under a court order or consent decree that mandates different procedures.

_____signature on file_____ _____

Robert E. Carter, Jr. Date

Commissioner