State of Indiana Indiana Department of Correction	Effective Date	Page 1 of	Number
	12/1/2020	9	04-05-102

POLICY AND ADMINISTRATIVE PROCEDURE
Manual of Policies and Procedures

Title
INTERNET, ELECTRONIC MAIL AND ONLINE IT SERVICES USE

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	04-05-101 04-05-103 through 04-05-109	IOT-CS-SEC-108

I. PURPOSE:

The purpose of this policy and administrative procedure is to establish security requirements for the appropriate use by authorized users of the Indiana Department of Correction (IDOC) pursuant to the Indiana Office of Technology (IOT) Acceptable Use of Information Technology Resources.

II. POLICY STATEMENT:

It is the policy of the Indiana Department of Correction (IDOC) to establish security requirements to protect all IDOC and IOT system assets assigned to authorized users in order to ensure business continuity, pursuant to Information Resources Use Agreement. This policy and administrative procedure shall be reviewed annually and updated when necessary.

III. DEFINITIONS:

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

A. 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 (IT) 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.

B. CLOUD COMPUTING: The “cloud” is a metaphor for the internet; therefore, cloud computing is a type of internet-based computing that utilizes shared internet resources, such as servers, applications, and storage, rather than local services or personal computing

devices. Cloud infrastructure is maintained by the cloud provider, not the individual cloud customer.

C. CLOUD FILE SHARING SOLUTIONS: Online, internet-based services in a cloud infrastructure that allow users to store and synchronize documents, photos, data, videos and other files, and share them with multiple users across multiple computing devices, such as desktops, notebooks, smartphones and media tablets.

D. EDISCOVERY: The production of files or other data held in an electronic form, such as e-mail, wherein "discovery" refers to the process of complying with legal obligations to produce relevant documents and information to opposing counsel in the course of civil litigation or to prosecutors or government investigators in criminal or regulatory proceedings.

E. INTERNET: A worldwide system of computer networks (a network of networks) in which computer users can get information and access services from other computers. The internet is generally considered to be public, untrusted, and outside the boundary of the State of Indiana enterprise network.

F. INTERNET FORUM: An online, internet discussion site where individuals can hold conversations in the form of posted messages. Examples include message and discussion boards and their associated threads, blogs and listserv applications.

G. NON-IDOC SYSTEM ACCESS: Non-IDOC IT access given to users whose duties, roles, responsibilities, or assignments require access to non-IDOC networks, data and/or services or resources.

H. OFFICE 365: Also called "Microsoft 365" or "Microsoft Office 365" is a Web-based version of the Microsoft Office suite of enterprise productivity applications, such as Exchange Online for e-mail and Skype for Business, provided to users through Cloud Computing infrastructure. Office 365 is a mission critical tool used by Authorized Users.

I. PEER-TO-PEER (P2P) FILE SHARING: The direct sharing of content like audio, video, data software or anything in digital format between two computers connected to a network without the need for a central server.

J. PERSONALLY IDENTIFIABLE INFORMATION (PII): Information that can be used directly or in combination with other information to identify a particular individual. PII includes: A name, identifying number, symbol, or other identifier assigned to a person. Any information that describes anything about a person. Any information that indicates

actions done by or to a person. Any information that indicates that a person possesses certain personal characteristics

K. PRIVILEGE USER ACCOUNTS: Passwords associated with user accounts, which are assigned to individuals (commonly referred to as named accounts), that have elevated access to make changes to system parameters. In IDOC, only Authorized Users authorized at a technical level to administer and support/maintain State computing IT systems and telecommunications technology systems are issued Privilege User Accounts.

L. REGULAR SYSTEM ACCESS: IDOC IT access given to users whose duties, roles, responsibilities, or assignments require access to basic, standardized IDOC system assets such as e-mail, offender management systems, and other resources required for job related duties.

M. SAVE PASSWORD OPTION: An option on some IT systems that, when enabled, allows the user to choose to have the user password retained within the system so that it will not have to be re-entered by the user upon subsequent access to the IT system.

N. SENSITIVE DATA: Any type of data that presents a high or medium degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a medium risk and potentially a high risk in cases for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The data may be certain types of PII that is also sensitive, such as medical information, social security numbers and/or financial account numbers. In addition, the data may be other types of information not associated with a particular individual such as security and infrastructure records, system administrative passwords, trade secrets, and business bank account information.

O. SENSITIVE SYSTEM ACCESS: IT access given to users whose duties, roles, responsibilities, or assignments require access to sensitive and controlled IDOC system assets.

P. SPECIALIZED SYSTEM ACCESS: IDOC IT access given to users above the regular system asset level whose duties, roles, responsibilities, or assignments require access to additional system assets.

Q. 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 IT 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.

R. TICKET: - The term commonly used by authorized IDOC users to describe a report of an IT incident, problem or issue or a request for a specific IDOC IT product or service.

IV. PROCEDURES:

A. System assets that contain data, text, images, or other information created, stored, transmitted, received, displayed or archived using IDOC or IOT resources are the property of IDOC and/or IOT except for those IT items whose ownership is protected by law, contract, license agreement, copyright, or other agreement. System assets are subject to review, investigation and inspection and, depending upon its content, may be subject to public records laws and/or eDiscovery. As a result, authorized users of system assets have no expectation of privacy.

B. IDOC and IOT can access and monitor the use of all system assets and generate and retain logs, reports, and other documentation pertaining to the use of the system assets. IDOC and IOT shall disclose usage logs and other documentation when deemed appropriate for purposes of litigation, audits, and investigations. Any suspected misuse of any system assets shall be reported in writing to the Executive Director of Technology Services who may, in turn, report the suspected misuse to the Office of Investigations and Intelligence for further investigation and action.

C. IDOC IT reserves the right to limit and restrict access to all system assets. In order to protect the security of said system assets, all access requests from IDOC authorized users shall be documented by submitting a ticket pursuant to Policy and Administrative Procedure 04-05-108, "Standardized Procedures to Report IT Incidents, Problems, Issues or Request Service," and shall be reviewed and approved by one (1) or more management levels as follows:

1. Regular System Access – the immediate supervisor of an IDOC authorized user, or appropriate supervisor if a non-IDOC authorized user, shall review and approve the request.

2. Specialized System Access – the immediate supervisor of an IDOC authorizer user, or appropriate supervisor if a non-IDOC authorized user, and the managing officer/designee shall review and approve the request.

3. Sensitive System Access – the immediate supervisor of an IDOC authorized user, or appropriate supervisor if a non-IDOC authorized user, and the managing officer/designee shall review and approve the request.

D. Approved System Access Requests shall be submitted by the final approving supervisor/manager/administrator to the IDOC Technology Services Helpdesk by submitting a ticket pursuant to Policy and Administrative Procedure 04-05-108. Upon receipt of the ticket and attached approval, IDOC Help Desk staff shall create the appropriate user account.

E. In order to obtain access to non-IDOC or non-IOT IT systems, networks, or data, such as the authorized users shall follow all access request, policies, and procedures of the external agency that owns, manages, or hosts the IT systems, networks or data.

F. Authorized users who receive access to any system assets shall follow all IDOC and IOT security requirements:

1. All system assets, including, but not limited to, all computing devices, the internet, electronic mail and the other tools in Office 365, all on-line services and resources, all telecommunications devices and services, all unified communications services, all digital devices, and virtual privacy network (VPN) access shall be used by authorized users for State of Indiana business purposes only.

2. Authorized users assigned any system asset shall not:

   a. Allow or permit any offender to use/access any system asset or view any content displayed on a system asset.

   b. Use any system assets to violate local, state or federal law or encourage the violation of local, State or federal law.

   c. Use any system asset to download, duplicate, disseminate, print, or otherwise use copyrighted materials (e.g., software, texts, music, graphics or other content) in violation of copyright laws.

   d. Use any system asset to operate a business, directly or indirectly, for personal gain or attach a signature on any electronic communications that contains information (i.e., name, title, and contact information) that is not related to State of Indiana business.

   e. Use any system asset to access or participate in any type of personals advertisements or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services, or other personals advertisements.

   f. Use any system asset to download, display, transmit, duplicate, store, or print any material that is sexually explicit, obscene, offensive, threatening, or harassing,

including disparaging or derogatory statements about others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.

g. Use any system asset to download, display, transmit, duplicate, store, or print any communications, including images, that contain incendiary statements which might incite violence or describe or promote the use of weapons or other devices associated with illegal activities.

h. Use any system asset to download, display, transmit, duplicate, store or print or otherwise organize any data or other materials, including images, used to wager on or participate in any type of gambling event or gambling game of chance or used for recreational purposes (i.e., playing computer games).

i. Use any system asset to solicit money or support on behalf of any religion or political cause.

j. Use a State business e-mail account for personal communications in internet forums.

k. Impede the State of Indiana's ability to access, inspect, and/or monitor any system assets including, but not limited to, inappropriately encrypting or concealing the contents of files or other electronic communications, inappropriately setting or manipulating system asset accounts or account passwords, physically concealing any device or tampering with, removing, or circumventing any security control put in place by IDOC or IOT to protect system assets.

l. Engage in any IT-related activities or actions that are unauthorized or outside one's job duties that could result in any IT security incident, as defined in Policy and Administrative Procedure 04-05-105, "Information Technology Security Incident Response," to include, but not limited to, unauthorized access to any system asset; denial of service (DoS) for any system asset; installation of malicious code on any system asset; improper usage or improper access to any system asset; scans, probes and attempted access of any system asset; information spillage for any system asset; loss or theft of any State of Indiana computing device or media, and the compromise, in any way, of any confidential, non-public and personally identifiable information (PII).

m. Conceal or misrepresent one's name, affiliation, duties, roles, responsibilities, or assignments in any electronic communications in order to obtain access to any system asset user account or in order to mask any unauthorized, illegal, fraudulent, irresponsible, or offensive behavior.

n. Access, download, display, transmit, duplicate, store, or otherwise disseminate any State sensitive data, confidential data or PII without the proper authorization.

o. Use a State business e-mail account or any non-State information system account for non-business purposes to access personal information, confidential information, or PII about an individual.

p. Disclose or share any System Asset passwords to/with any other individual, which includes posting or attaching passwords in writing anywhere in the work location, including on computing devices, where they can be viewed by others.

q. Use another authorized user's system asset account or signature line without proper authorization.

r. Use a "save password" option on any system asset.

s. Use the same password for any system asset privilege user accounts and any other system asset user accounts.

t. Set, manipulate, deactivate, or disable any authorized user's system asset password or user account to impede access to the system asset, without proper authorization.

u. Use any system asset to engage in peer-to-peer (P2P) file sharing with an external, non-business computer system or network.

v. Use any system asset account to order, download, display, transmit, duplicate, or store any non-IDOC or non-IOT authorized software, software service packs, or software updates for use with/on any system asset.

w. Use a system asset to send unsolicited e-mail or facsimile communications in bulk or forward electronic chain letters in bulk to recipients inside or outside the State of Indiana business environment.

x. Download, install, and/or use a personal, privately-owned, or consumer-grade e-mail or unified communications account on any system assets to conduct State business.

y. Physically relocate or replace any non-mobile State computing hardware/equipment assigned to end users (i.e., PCs or network printers) without the approval of the authorized user at a technical level at the IDOC facility/office who is responsible for administering and supporting/maintaining the facility/office's State computing IT systems and telecommunications technology systems.

3. Authorized users shall adhere to the following internet access requirements:

   a. Authorized users shall use system assets to access internet resources required to perform assigned job duties.

   b. Authorized users with a business-related need to use system assets to access internet resources restricted by IOT shall:

      1) Submit a written e-mail request to the immediate supervisor, if an IDOC authorized user, or to the appropriate non-IDOC supervisor if a non-IDOC authorized user. The email request shall contain the specific internet resource requested and the business justification for access the site.

      2) If the request is approved, the immediate/appropriate supervisor shall forward the request and business justification, via e-mail, to the appropriate managing officer for the facility or office for review.

      3) If the managing officer approves the request, the request shall be forwarded via e-mail to the Information Security Manager and Executive Director of Research and Technology who shall give the authorized user access to the site.

   c. IDOC employee, contractor, temporary employee or other agent of the State shall not:

      1) Design a personal social media site or channel or use a personal social media account to speak on behalf of, speak for, or otherwise represent the State or IDOC without the express authorization of the appropriate IDOC managing director.

      2) Use a social media account approved for a business-related need and accessed through system assets or a personal social media account to access, download, display, transmit, duplicate, store or otherwise disseminate any State data or information that is not classified as public information.

   d. Authorized users shall not include pointers or references to any personal social media account in any system asset account (i.e., including a social media account reference or pointer in a State e-mail account signature line).

   e. Authorized users of system assets shall use only the Cloud File Sharing Solutions approved by IDOC or IOT to store or share State data or synchronize State data between multiple computing devices. Authorized users shall not use approved Cloud File Sharing Solutions to:

1) Store or share personal data or information or any other personal content; and,
2) Store or share PII, sensitive or confidential State data, information, or other content without the approval of the appropriate managing director.

4. When any authorized user assigned a desktop or laptop computer leaves the physical proximity of their work area, the authorized user shall secure the computer to prevent unauthorized access to the device or its data/information, using one or more of the following methods:

   a. Log off all accounts, including the computer and/or network account;
   b. Lock the computer by using an approved password protected screensaver;
   c. Lock the computer by using operating system level workstation locking;
   d. Shut the computer down.
   e. For laptop computers, physically secure the system to prevent removal.

5. When an authorized user has reason to believe any system asset or the password integrity of any system asset has been compromised in any way, the authorized user shall notify in writing the Executive Director of Technology Services.

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