OFFICE OF THE SECRETARY OF STATE
LAVONNE GRIFFIN-VALADE
SECRETARY OF STATE

CHERYL MYERS
DEPUTY SECRETARY OF STATE
AND TRIBAL LIAISON

ARCHIVES DIVISION
STEPHANIE CLARK
DIRECTOR

800 SUMMER STREET NE
SALEM, OR 97310
503-373-0701

NOTICE OF PROPOSED RULEMAKING
INCLUDING STATEMENT OF NEED & FISCAL IMPACT

CHAPTER 291
DEPARTMENT OF CORRECTIONS

FILED
02/29/2024 12:13 PM
ARCHIVES DIVISION
SECRETARY OF STATE

FILING CAPTION: INFORMATION SYSTEMS ACCESS AND SECURITY

LAST DAY AND TIME TO OFFER COMMENT TO AGENCY: 04/18/2024 5:00 PM

The Agency requests public comment on whether other options should be considered for achieving the rule's substantive goals while reducing negative economic impact of the rule on business.
A public rulemaking hearing may be requested in writing by 10 or more people, or by a group with 10 or more members, within 21 days following the publication of the Notice of Proposed Rulemaking in the Oregon Bulletin or 28 days from the date the Notice was sent to people on the agency mailing list, whichever is later. If sufficient hearing requests are received, the notice of the date and time of the rulemaking hearing must be published in the Oregon Bulletin at least 14 days before the hearing.

CONTACT: Julie Vaughn	3601 State St	Filed By:
971-701-0139	Salem,OR 97301	Julie Vaughn
Julie.A.VAUGHN@doc.oregon.gov		Rules Coordinator

NEED FOR THE RULE(S)

These rules establish policies, procedures, and guidelines for the security of Department of Corrections information systems. These revisions better reflect and implement the direction of the agency, statewide standards, and industry modernization; improve consistency and clarity of the rules; further define and update process; update position titles and timelines; and establish guidelines around separation of duties, authorizing access, shared or group credentials, and open user accounts, and physical security.

DOCUMENTS RELIED UPON, AND WHERE THEY ARE AVAILABLE

Common Platform Enumeration: Naming Specification Version 2.3 released by the U.S. Department of Commerce through the National Institute of Standards and Technology (NIST) found:
https://nvlpubs.nist.gov/nistpubs/legacy/ir/nistir7695.pdf

STATEMENT IDENTIFYING HOW ADOPTION OF RULE(S) WILL AFFECT RACIAL EQUITY IN THIS STATE

The Department of Corrections (DOC) anticipates that the proposed amendments made to the Network Information Systems Access and Security rules (OAR 291-005) will have no impact on racial equity in the State of Oregon.
These rules establish the policies, procedures, and guidelines for the security of Department of Corrections information systems which includes any information system operated by the Department of Corrections, connected to the department's network, or information contained in Department of Corrections computer systems. Among the proposed amendments to the rules are changes to align OAR 291-005 with modern legislation, regulatory requirements, and industry standards by modernizing definitions, outlining the requirements for access and security, and providing a framework for user identification and credential management. These rules have not been updated since 2000 so these technical corrections amend the rules to reflect current processes, practices, and terminology. Internal department responsibilities were expanded, but no major operational or policy changes were made. These rules have no direct application to adults in custody and any previous reference related to adults in custody (or “inmate”) has been stricken

from these rules. For these reasons, the department anticipates that these proposed rule amendments will have no impact on racial equity in this state.

FISCAL AND ECONOMIC IMPACT:

Rule 291-005 is updated to better reflect and implement the direction of the agency, statewide standards, and industry modernization as it relates to information systems within DOC. The changes are not anticipated to have a fiscal impact on DOC, AICs, other state agencies, local governments (the counties), or the general public.

COST OF COMPLIANCE:

(1) Identify any state agencies, units of local government, and members of the public likely to be economically affected by the rule(s). (2) Effect on Small Businesses: (a) Estimate the number and type of small businesses subject to the rule(s); (b) Describe the expected reporting, recordkeeping and administrative activities and cost required to comply with the rule(s); (c) Estimate the cost of professional services, equipment supplies, labor and increased administration required to comply with the rule(s).

None.

DESCRIBE HOW SMALL BUSINESSES WERE INVOLVED IN THE DEVELOPMENT OF THESE RULE(S):

Small businesses were not involved in the development of these rules as they will not be impacted by these rules.

WAS AN ADMINISTRATIVE RULE ADVISORY COMMITTEE CONSULTED? NO IF NOT, WHY NOT?

The department has determined that use of an advisory committee would not have provided any substantive assistance in drafting these rule revisions because of the technical nature of the revisions.

RULES PROPOSED:

291-005-0005, 291-005-0011, 291-005-0015, 291-005-0025, 291-005-0035, 291-005-0045, 291-005-0055, 291-005-0065, 291-005-0075

AMEND: 291-005-0005

RULE SUMMARY: Amends rule to better reflect and implement the direction of the agency, statewide standards, and industry modernization; to make changes for consistency throughout the rule; and for clarity.

CHANGES TO RULE:

291-005-0005
Authority, Purpose, and Policy ¶

(1) Authority: The authority for th~~is~~ese rules is granted to the Director of the Department of Corrections in accordance with ORS 179.040, 423.020, 423.030, and 423.075.¶

(2) Purpose:¶

(a) The purpose of th~~is~~ese rules is to establish policies, procedures, and guidelines for the security of Department of Corrections ~~(DOC)~~ information systems. Any information system operated by the Department of Corrections ~~or~~, connected to the department's network ~~and~~, or information contained in ~~DOC information networked~~the department's computer systems shall be protected by the security guidelines established in th~~is~~ese rules.¶

(b) The Department of Corrections intends to operate all ~~of its automation resource~~information system assets, including multi-user computer systems, terminal devices, ~~personal computers (PCS),~~ work-stations, networks, mobile devices, and communications devices, in such a manner as to ensure:¶

(A) The ~~accuracy and reli~~confidentiality, integrity, and availability of the department's information, regardless of whether it is stored ~~and~~or processed on the department's information systems or on other computer systems, including employee-owned personal computers or information systems operated by other agencies and organizations;¶

(B) The protection of ~~each individual's~~ rights t~~of~~ privacy concerning personally identifiable information (PII) about

~~that~~a person which may be stored on D~~OC~~epartment of Corrections information systems;¶
(C) Accessibility to ~~the~~ information by department-authorized users o~~f DOC information systems~~r as required by state statute or legislation;¶
(D) Denial of access to D~~OC~~epartment of Corrections information systems and information contained within for all ~~other~~ unauthorized persons; and¶
(E) Detection of ~~and~~misuse of Department of Corrections information systems, computer equipment, computer networks or information, and the intervention ~~in~~against attempted or actual system ~~break-i~~intrusions, information tampering ~~and~~, destruction, ~~and all other forms of misuse of DOC information systems, computer equipment, computer netw~~data exfiltration, or any other for~~k~~ms ~~and information~~of misuse.¶
(3) Policy: It is the policy of the Department of Corrections that computerized information shall be made secure from unauthorized access. Accepted supervision and management practices shall be required of employees to provide adequate security which restricts unauthorized access. Any external organization granted access to D~~OC~~epartment of Corrections information systems shall be required to follow and enforce the security guidelines of these rules.
Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

AMEND: 291-005-0011

RULE SUMMARY: Amends rule to better reflect and implement the direction of the agency, statewide standards, and industry modernization.

CHANGES TO RULE:

291-005-0011
Definitions ¶

(1) A~~ccount/User Profile: A data record which is associated with each authorized user of a computer system and/or network. This record specifies the user's real name, log-on or sign-on name, secret password, identification numbers or codes, and other operating parameters (such as limitations on the use of system resources, access permissions, etc.). This record is created and maintained for each user by the DOC network security officer or his/her designee. The record is used by the computer or network operating system software to permit or deny use of or access to system resources for a given user.¶~~
~~(2) Application(s): Any computer program or group of related computer programs which perform specific operations to support or execute information processing required by the user or department~~pplication(s): A system for collecting, saving, processing, and presenting data by means of a computer. The term application is generally used when referring to a component of software that can be executed. The terms application and software application are often used synonymously.¶
(~~3~~2) Authorized User: An individual who holds explicit permission to access information or use an information systems resource. An authorized user is distinguished by ownership of an active user account~~/use ~~or profile and a fully executed security agreement.¶
(~~4~~3) Com~~munications~~puting Devices: A~~ny equipment which supports the connection of an information processing component (for example, a terminal, PC, or host computer) to another information processing component for the purpose~~ device that can perform substantial computations, including numerous arithmetic operations and logic operations without human intervention. A computing device can consist of ~~data transmission and reception.¶~~
~~(5) Computer Equipment: Automation resources including, but not limited to, terminals, personal computers, work stations, controllers, printers, and communications devices.¶~~
~~(6) Dial-up: Access to a computer system or network which uses communications devices. For instance, a user might use a PC and modem from home to review a department report which is stored on a minicomputer; a user who is traveling can use a laptop PC with a modem to send and receive electronic mail from his/her hotel roo~~a standalone unit or several interconnected units. It can also be a device that provides a specific set of functions, such as a phone or a personal organizer, or more general functions such as a laptop or desktop computer.¶
(4) Department of Corrections Information Security Officer (ISO): The ISO manages information security throughout the agency. The ISO is responsible for coordinating program requirements throughout the agency with designated points of contact and project managers. Their duties include:¶
(a) Developing and maintaining an agency-wide information security program.¶
(~~7~~b) ~~DOC Network Security Officer: A person(s) appointed by the Assistant Director~~Issuing annual information technology (IT) security planning guidance, including security priorities, objectives, and prioritization criteria for new and legacy systems.¶
(c) Training and overseeing personnel with significant responsibilities for ~~I~~information ~~Systems and Services Division (ISSD) to perform security functions for the DOC information system~~security with respect to such responsibilities.¶
(d) Developing and maintaining information security policies, procedures, and control techniques.¶
(e) Assisting senior agency personnel concerning their IT security-related responsibilities.¶
(~~8~~5) External organization: Any non-Department of Corrections department, agency, corporation, or other group~~s~~ of individuals who are not under the authority of the ~~Director of the~~ Department of Corrections Director. This includes, but is not limited to, national, state, county, and municipal government agencies and departments, service providers and consultants, product and services vendors, appointed or ad hoc committees, advisory groups, and the public at large.¶
(~~9~~6) Functional Unit: Any organizational component within ~~the~~ Department of Corrections responsible for the delivery of program services or coordination of program operations.¶
(~~10~~7) Functional Unit Manager (FUM): Any person within ~~the~~ Department of Corrections who reports to either the Director, the Deputy Director, an Assistant Director, or an administrator and has responsibility for delivery of program services or coordination of program operations.¶
(~~11~~8) Information System: A~~ny automated system which supports storage, processing of and access to information (data). An~~ discrete or interconnected set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system ~~includes the physical~~

~~equipment, software, and data.¶~~

~~(12) Inmate: Any person under the supervision of the Department of Corrections or other c~~normally includes hardware, software, information, data, applications, and communications.¶

(9) Mobile Device: A portable computing device that has a small form factor such that it can easily be carried by a single individual, is designed to operate without a physical connection, possesses local, non-removable or re~~ctions agency who is not on parole, probation, or post-prison supervision statu~~movable data storage, and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, or built-in features that synchronize local data with remote locations.¶

(1~~3~~0) ~~Offender: Any person under the supervision of local community corrections who is on parole, prob~~Multi-Factor Authentication (MFA): An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination~~, or post-prison supervision status~~f authenticators that provide different factors. These factors include something you know, something you have, and something you are.¶

(1~~4~~1) Oregon Corrections Enterprises (OCE): A semi-independent state agency that is a non-Department of Corrections agency or division, which is under the authority of the ~~Director of the~~ Department of Corrections Director. For purposes of this rule only, Oregon Corrections Enterprises shall not be considered an external organization.¶

(1~~5~~2) ~~Oregon Corrections Enterprises (OCE) Employee: Any person employed full-time, part-time, or under temporary appointment by the Oregon Corrections Enterprises. For the purposes of this rule only, employee shall also include any person under contractual arrangement to provide servi~~Personally-Owned Devices: Any technology device that was purchased by an individual and was not issued by the agency.¶

(13) Privileged Account: An account provided to a privileged user for performing administrative or security-relevant functions.¶

(14) Privileged User: A user that is authorized, and therefore trusted, to perform security-relevant functions that ordinary users are not authorized to perform.¶

(15) Remote Access: Access to ~~the agency; any person employed by private or public sector agencies who is serving under agency-sanctioned special assignment to provide services or support to agency programs~~an organizational information system by a user or an information system communicating through an external, non-organization-controlled network (e.g., the Internet).¶

(16) Stand-alone ~~Personal~~ Computer Equipment: Computer equipment not connected to ~~the Department of Corrections network or any other network~~any network.¶

(17) Telework or Telecommuting: The ability of staff to conduct work from locations other than regularly assigned agency facilities.¶

(1~~7~~8) Terminals: Input~~/~~ and output devices that are used for data entry and display of entered or processed information. A terminal consists of a display screen and some form of input device, usually a keyboard or scanner.¶

(19) User Account or Profile: A data record associated with each authorized user of a computer system or network. This record specifies the user's real name, username, encrypted password, identification numbers or codes, and other operating parameters (such as limitations on the use of system resources, access permissions, etc.). This record is created and maintained for each user by the Department of Corrections Profile Administration Team. The record is used by the computer or network operating system software to permit or deny use of or access to system resources or information assets for a given user.

Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075

Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

AMEND: 291-005-0015

RULE SUMMARY: Amends rule to better reflect and implement the direction of the agency, statewide standards, and industry modernization; for clarity and to further define process.

CHANGES TO RULE:

291-005-0015
General ¶

(1) These rules cover the following assets of the department:¶
(a) Any and all information regarding or related to the department's business and mission, where that information is stored as data contained in or on any information system~~,~~ or is produced for display and review by that system.¶
(A) ~~Such d~~Data may be recorded on ~~a number of~~ different media, such as magnetic ~~tapes, magnetic or optical disks, hard or floppy disks, CD ROM~~drives (hard disk drive (HDD) or floppy), optical disks (compact disk (CD) or digital versatile disk (DVD), semiconductor drives (solid state drives (SSD) or flash), and a variety of printed ~~forms on paper~~output, etc.¶
(B) This data may be stored, processed, accessed, ~~and~~or displayed on any number of computer systems including, but not limited to, those owned and operated by the department,~~ its employees,~~ contractors, ~~and~~or consultants. Personally-owned devices are not authorized to store or process agency data.¶
(b) The information systems equipment, ~~specifically~~including the computer hardware and software, peripheral devices, network components, data communications devices, terminals, ~~personal~~stand-alone computers, and printers which are owned, leased~~ and/~~, managed, or operated by the department to collect, store, process, ~~and~~maintain, disseminate, dispose of, or display information.¶
(c) Access to and use of the department's information systems.¶
(2) These rules ~~specify the means to detect and prevent misuse and/or loss of any of these assets. It covers the range of misuse from innocent accidents which cause little or no damage to malicious actions which cause data corruption, loss of i~~enable the agency to mitigate the potential loss of data from misuse of user accounts. Further prevention, mitigation, and remediation efforts are explained in agency policies and procedures as well as the State of Oregon Security Plan and State of Oregon Information~~,~~ and ~~denial of service~~Cyber Security Standards.
Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

AMEND: 291-005-0025

RULE SUMMARY: Amends rule to better reflect and implement the direction of the agency, statewide standards, and industry modernization; to further define process; and for consistency with other department rules.

CHANGES TO RULE:

291-005-0025
Access Authorization ¶

(1) Only authorized users shall be allowed access to D~~OC~~epartment of Corrections information systems.¶
(2) Authorized users shall be granted access to D~~OC~~epartment of Corrections information systems on a need-to-use basis. Such access will be controlled by ~~use of~~ a password. MFA will be required in some instances to access agency information systems.¶
(3) Requests for user access and termination of user access shall be accepted by the D~~OC network security officer~~epartment of Corrections ISO or designee from functional unit managers or their designees only. These personnel shall handle all requests for access and termination for their functional unit. Letters of agreement with external organizations for access to D~~OC~~epartment of Corrections information systems shall clearly indicate the process and authority for user access authorization. Users from external organizations must comply with this rule.¶
(4) No person presently or previously under the custody, control, or supervision of ~~the~~ Department of Corrections or its agents shall be granted access to any computers or systems which contain data or are connected to any D~~OC~~epartment of Corrections information system unless the request for access has been ~~reviewed, approved and~~ recommended by the functional unit manager to the ISO for review and initial approval. Final approval for such access will be determined by the Assistant Director ~~for ISSD~~of Administrative Services.¶
(5) Functional unit managers or their designees shall identify their staff who have a need to use D~~OC~~epartment of Corrections information systems and shall be responsible for the following process for authorization:¶
(a) Functional unit managers or their designees are responsible to ensure that criminal history checks and Criminal Justice Information Systems (CJIS) clearance checks have been done on all persons for whom they request authorization to access D~~OC~~epartment of Corrections information systems. This includes contractors, volunteers, temporary staff, regular employees, and OCE employees.¶
(b) Security Agreement:¶
(A) All persons requesting access to D~~OC~~epartment of Corrections information systems must sign a security agreement which indicates that they understand they are responsible to protect agency assets, including computers and information, in accordance with the ~~provisions of the Department of Correction~~department's rules on ~~R~~release of ~~P~~public ~~I~~information; ~~F~~files, ~~R~~records, and ~~D~~detainers; and ~~N~~network and ~~I~~information ~~S~~system ~~A~~access and ~~S~~security.¶
(B) ~~The DOC network security officer or designee shall maintain a file of security agreements~~Security agreements are to be maintained within each staff member's employee file.¶
(c) Authorization Form:¶
(A) The user's functional unit manager or designee shall complete an authorization form requesting access to ~~the DOC~~any Department of Corrections network, a~~nd the DOC application~~pplication, folder, or asset including modification of such access.¶
(B) A separate request form shall be completed if the user is requesting ~~dial-up access to DOC information system~~approved telework access.¶
(C) Authorization forms shall be signed by the functional unit manager or designee for the functional unit or external organization and shall be forwarded to the D~~OC network security officer who shall generate a user identification and a user account allowing the access request~~epartment of Corrections ISO or designee who shall generate a user account allowing the access requested. The Department of Corrections ISO or designee shall notify the user when the profile is activated and access is authorized.¶
(d) Training: The user shall be required to complete ~~a training module on password management before access to the system is authorized~~information security training within 30 days of account creation. Notification of completion of training shall be forwarded to the D~~OC network security officer or designee, who shall then activate the user's profile. The DOC network security officer shall notify the user when the profile is activated and access is authorized~~epartment of Corrections ISO or designee. Account access will be disabled if the required training module(s) are not completed within the allotted 30 days.
Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

AMEND: 291-005-0035

RULE SUMMARY: Amends rule to better reflect and implement the direction of the agency, statewide standards, and industry modernization; update change in practice around transfers and position titles; extend timeline for removal of newly created user profiles; and update and clarify timelines.

CHANGES TO RULE:

291-005-0035
Termination of Access ¶

(1) Notice of termination of employment ~~or a transfer to a position not requiring access under these rules~~with the agency shall result in retirement of the individual's user ~~identification~~account(s). Prompt notice of termination ~~or transfer ~~shall be sent to the D~~OC network security officer by the functional unit~~epartment of Corrections ISO or designee by the Employee Services manager or designee who handles user authorization. This procedure also applies to users from external organizations~~ and~~, Oregon Corrections Enterprises, contractors, and volunteers.¶
(2) Functional unit managers or their designees shall review ~~annually for accuracy ~~a list of user accounts from their respective units~~. The~~ annually to ensure accounts are legitimate. Information ~~Systems and~~Technology Services ~~Division (ISSD~~(ITS) shall provide the list.¶
(3) Managers of external users shall review a list of users annually and confirm those needing continued access. ITS~~SD~~ shall provide the list.¶
(4) Newly~~-~~ created user profiles that are not used within ~~three weeks will be disabl~~45 days will be removed.¶
(5) User profiles for deceased employees shall be immediately disabled upon notification. Notification is provided to manager and site contact. If no response is received from the manager or site contact within 14 days, the profile will be deleted.¶
(~~5~~6) ~~Own~~Users and managers of existing profiles that are ~~not used~~inactive for a period of ~~three month~~45 days will be sent ~~a letter by the DOC network security officer~~notification by the Department of Corrections ISO or designee to confirm continued need for access. If there is no response within 10 business days, the profile will be disabled~~ after six mo~~. Disabled account~~h~~s ~~of inactivity.¶~~
~~(6) Passwords that have been disabled for a perio~~will be deleted 30 days after disablement, unless otherwise noted o~~f~~n th~~ree months will be deleted~~e account.
Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

AMEND: 291-005-0045

RULE SUMMARY: Amends rule to better reflect and implement the direction of the agency, statewide standards, and industry modernization.

CHANGES TO RULE:

291-005-0045
~~Dial-Up~~Remote Access ¶

(1) Authorized persons may be granted access to D~~OC~~epartment of Corrections information systems by means of ~~dial-up~~remote connection on a need-to-use basis. Such access shall be via the same user identification and password issued for ~~non-dial-up~~local access.¶
(2) ~~Dial-up~~Remote access is permitted by means of user identification and password only. The use of open user accounts and automatic sign-on are not permitted.¶
(3) ~~No inmate/offender shall be permitted to access DOC information systems by means of dial-up connection.¶~~
~~(4) The ISSD standards and guidelines require additional~~ITS standards and guidelines require additional security controls, such as MFA, virtual private network (VPN), geolocation verification, or other forms of securi~~ty~~e con~~trols~~nection to be used whenever ~~dial-up access~~telecommuting is authorized.
Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

AMEND: 291-005-0055

RULE SUMMARY: Amends rule to better reflect and implement the direction of the agency, statewide standards, and industry modernization; to further define process and clarify rule; and to add training timeline.

CHANGES TO RULE:

291-005-0055
User Password Management and Responsibilities ¶

(1) Authorized users shall comply with the following rules to create and manage their passwords:¶

(a) All user accounts shall be protected by use of a password. This password shall be generated by and known only to the individual user.¶

(b) The D~~OC network security officer~~epartment of Corrections ISO shall determine password characteristics.¶

(2) Password Duration: All user passwords shall be subject to automatic retirement at a maximum set time period in the standards and guidelines. Authorized users may change passwords as often as they wish during this period and are encouraged to do so.¶

(3) Password Violation: Violation of these rules is a disciplinary matter~~,~~ with consequences up to and including dismissal~~ as a consequence~~.¶

(4) A user account shall be automatically disabled when there have been more than ~~three successive unsuccessful attempts at sign-on.¶~~

~~(5) The DOC network security officer or designee may re-enable a disabled password.¶~~

~~(6) Personal Computer Network Access: Personal computers (PCs) which connect to the local or wide area network for the purpose of accessing and using file, disk, application, and printer services must be treated with the same care and diligence accorded to terminals connected directly to a computer system. Such PC connections must be mediated by the user's log-on name an~~five consecutive invalid logon attempts by a user during a 120-minute time period.¶

(5) The Department of Corrections ISO or designee may re-enable a disabled password.

Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

AMEND: 291-005-0065

RULE SUMMARY: Amends rule to better reflect and implement the direction of the agency, statewide standards, and industry modernization through guidelines around separation of duties, authorizing access, shared or group credentials, and open user accounts.

CHANGES TO RULE:

291-005-0065
Information ~~Systems and~~Technology Services ~~Division (ISSD~~(ITS) Responsibilities for User Identification-
To implement user accountability, the following rules shall be strictly enforced by I~~SSD~~TS:¶
(1) Separation of Duties:¶
(~~1~~a) ~~The same user identification (numeric value and/or user name) shall not be assigned to more than one user~~Separate personnel duties to minimize the potential for abuse of authorized privileges and risk of malevolent activity without collusion. Developers must not have unmonitored access to production environments;¶
(b) Document separation of duties, including roles and permissions; and¶
(c) Define system access authorization in support of separation of duties.¶
(2) Employ the principle of least privilege allowing only authorized access for users, or processes acting on behalf of users, which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.¶
(a) Authorize Access to Security Functions:¶
(A) Explicitly authorize access to administrative privileges, including security functions and security relevant information; and¶
(B) Establish procedures to maintain documentation of privileged access, including any elevated privileges, and privileges that provide administrative access to network devices, operating systems, software application capabilities, or scripting tools.¶
(b) Use of Non-privileged Access for Non-privileged Functions: Require that users of system accounts or roles, even those with access to privileged or administrative functions, use non-privileged accounts or roles when accessing systems for non-privileged or non-security functions.¶
(~~2~~c) ~~Group accounts are not allowed. A group account is a log-on or sign-on user name and password which is shared by more than one person~~Privileged Accounts: Restrict privileged accounts to authorized individuals with a need for elevated privileges.¶
(d) Review of User Privileges:¶
(A) Ensure that privileges assigned to users are reviewed to validate the need for such privileges:¶
(i) Initially upon hire;¶
(ii) Any time assigned job duties change;¶
(iii) Any time there is a change in job position;¶
(iv) Annually thereafter.¶
(B) Reassign or remove privileges as necessary, to correctly reflect organizational mission and business needs.¶
(e) Audit the Execution and Use of Privileged Functions.¶
(f) Prohibit Non-privileged Users from Executing Privileged Functions: Prevent non-privileged users from executing privileged functions including disabling, circumventing, or altering implemented security safeguards and countermeasures.¶
(3) Shared or Group Account Credentials: Shared or group account credentials must be changed when members leave the group.¶
(~~3~~4) Open user accounts are not allowed. An open user account is a log-on user-name for which there is no password, or for which the password is publicly known.
Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

AMEND: 291-005-0075

RULE SUMMARY: Amends rule to better reflect and implement the direction of the agency, statewide standards, and industry modernization through guidelines for physical security of computer equipment, physical access control, and evaluation and development of physical security guidelines.

CHANGES TO RULE:

291-005-0075
Physical Security Guidelines ¶

(1) Computer equipment shall be protected from unnecessary risk of access, damage, or theft.¶
(2) ~~An annual evaluation of physical security for AS400 computer s~~Facility access must be controlled using physical access control devices such as keys, locks, combinations, radio-frequency identification (RFID) card readers, etc.¶
(a) All facilities must have at least one physical security control protecting it from unauthorized access, damage, or interference;¶
(b) Facilities ~~s~~tha~~ll be conducted by AS400 system operators. The findings of this evaluation shall be reported by the system operators to the work group~~t process or store information classified at Level 3 (Restricted) or higher must employ multiple layers of physical security controls; and¶
(c) For areas used to process or store information classified at Level 3 (Restricted) or higher, access logs for controlled entry points must be maintained.¶
(3) An annual evaluation of physical security for ~~computer equipment used by their respective~~information systems used by staff shall be conducted by the ~~functional unit managers or their designees, who are i~~Department of Corrections ISO or their designee. The findings of this evaluation ~~c~~sha~~rge of user authorization~~ll be used to enhance the physical security of the agency systems as needed.¶
(4) Physical security guidelines for ~~AS400 sites and computer equipment~~information systems shall be developed by ITS~~SD~~ and reviewed and approved by the ~~automation security officer~~Department of Corrections ISO.
Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075