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
06/26/2024 2:48 PM
ARCHIVES DIVISION
SECRETARY OF STATE

FILING CAPTION: AIC Access to Automation

LAST DAY AND TIME TO OFFER COMMENT TO AGENCY: 08/16/2024 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
971-701-0139
julie.a.vaughn@doc.oregon.gov

3723 Fairview Industrial Drive SE #200
Salem,OR 97302

Filed By:
Julie Vaughn
Rules Coordinator

NEED FOR THE RULE(S)

The purpose of these rules is to establish Department of Corrections policies and procedures for authorizing adults in custody (AICs) access to and use of certain approved information technology while incarcerated in a Department of Corrections facility, and for appropriate supervision and management standards and practices to ensure adequate security safeguards for the same. These revisions update these rules to better reflect and implement the direction of the agency by changing the term "inmate" to "adult in custody (AIC)" and to better reflect statewide standards and industry modernization; expand and clarify the department's policy on AIC access to information technology; update definitions; adopt new rules concerning management of approved information technology, approval processes for requesting information technology to assist with a disability, and for the review and removal of access restriction; and reorganize these rules.

DOCUMENTS RELIED UPON, AND WHERE THEY ARE AVAILABLE

None.

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

The Department of Corrections anticipates that the proposed amendments to its Adult in Custody Access to Information Technology rules (OAR 291-086) will have an overall positive impact on racial equity in the State of Oregon. These rules establish the department’s policies and procedures for authorizing adults in custody access to and use of certain approved information technology while incarcerated in a Department of Corrections facility, and for appropriate supervision and management standards and practices to ensure adequate security safeguards for the same. The purpose of these rule changes is to update the agency’s policy on Information Security and access to Information Technology, aligning with modern legislation, regulatory requirements, and industry standards. These rules have not been updated since 2005 so these technical corrections amend the rules to reflect current processes, practices, and terminology.

These rule changes modernize definitions, outline the requirements for access and security, and create a framework for providing services to adults in custody. These changes provide more opportunity for adults in custody to access tools that are beneficial to their rehabilitation and reduces recidivism. Other than improving access for adults in custody, no major operational or policy changes were made.
Among the proposed amendments to Oregon Administrative Rule 291, Division 86, are amendments that will conform the rules to incorporate the new statutory term for individuals incarcerated in Department of Corrections institutions – "adult in custody," and reflect changes in the way Department of Corrections staff address and refer to individuals who are incarcerated in Department of Corrections institutions. The Department of Corrections understands that all adults in custody, including minority racial groups, are positively impacted when a culture of inclusivity, normalization, and humanization is created, and that these proposed rule amendments represent another step toward creating this culture. Because minority racial groups have historically been overrepresented among individuals who have been sentenced to prison incarceration in this state, the Department of Corrections anticipates that these proposed rule amendments will help promote the just and fair treatment of members of these groups while they are incarcerated in Department of Corrections correctional facilities, and upon their release and transition back into Oregon's communities upon completion of their incarceration sentences.
For the above reasons the department anticipates that these proposed rule amendments will have a positive impact on racial equity in this state.

FISCAL AND ECONOMIC IMPACT:

Rule 291-086 include updates to reflect and implement the direction of the agency, statewide standards, and industry modernization relating to AIC Access to Information Technology.

The changes are not anticipated to have an impact on DOC, AIC's, 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:
291-086-0010, 291-086-0020, 291-086-0030, 291-086-0036, 291-086-0040, 291-086-0045, 291-086-0046, 291-086-0047, 291-086-0049, 291-086-0050, 291-086-0060, 291-086-0070, 291-086-0071

AMEND: 291-086-0010

RULE SUMMARY: Amends rule to clarify and further define Policy and Purpose statements; and to update terminology..

CHANGES TO RULE:

291-086-0010
Authority, Purpose, and Policy ¶

(1) Authority: The authority for th~~is~~ese rules is granted to the Director of the Department of Corrections (DOC) in accordance with ORS 179.040, 423.020, 423.030 and 423.075.¶
(2) Purpose: The purpose of these rules is to establish ~~the approval process and set standards that allow inmat~~Department of Corrections policies and procedures for authorizing adults in custody (AICs) access to and use of certain approved information technology while incarcerated in a Department of Corrections facility, and for appropriate supervision and management standards and practices to ensure adequate security safeguards for the same.¶
(3) Policy:¶
(a) Access to ~~use computer equipment in the normal course of their work o~~and use of information technology in Department of Corrections facilities is increasingly important for AICs to access and participate in education programs, Career and Technical Education (CTE) programs, reentry programs, work programs, food services, law library services, general library services, recreation programs, and other programs ~~assignment~~and facility operations, and for successful transition into the community upon release from incarceration.¶
(~~3~~b) ~~Policy: It is the policy of the Department of Corrections that security not be compromised by inmate use of computer equipment. Inmate use of computer equipment shall not jeopardize~~Accordingly, within the inherent limitations of resources and the need for facility security, safety, health, and good order, it is the policy of the Department of Corrections to authorize AICs to access and use approved information technology while incarcerated in Department of Corrections facilities in accordance with these rules.¶
(c) When authorized by the department, AIC access to and use of approved information technology is permitted neither as a matter of right nor as a privilege of the AIC; rather, AIC access to and use of information technology may be authorized when in the judgment of the department it furthers the AIC's programming and rehabilitation, the department's correctional goals and mission, and is consistent with the safe~~ty~~, secur~~ity or~~e, orderly, and efficient management and operation of ~~any~~ Department of Corrections facilit~~y.~~ies.¶
(d) Appropriate supervision and management practices associated with AIC access to and use of approved information technology shall be maintained at all times to ensure adequate security safeguards.
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: 291-086-0020

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

CHANGES TO RULE:

291-086-0020
Definitions ¶

(1) ~~Computer Equipment: Any automated processing or data storage devices including, but not limited to, personal computers, work st~~Adult in Custody: Any person under the custody or supervision of the Department of Corrections and who is not on parole, probation, or post-prison supervision.¶
(2) AIC Supervisor: Any employee of the Department of Corrections or of Oregon Corrections Enterprises (OCE), or any DOC or OCE contractor, that is responsible for supervising an AIC.¶
(3) Approved Information Technology: Any information technology that has, through proper procedure, been requested, verified, vetted, and approved by the Assistant Director of Operations or their designee and the Chief Information Officer or their designee. Approved information~~s, terminals, controllers, printers, and communication devices.¶~~
~~(2) Department of Corrections (DOC~~chnology may include the material physical components or logical software components of an information system for the use of education, CTE, reentry, work, food services, law library, general library, recreation, or other programs.¶
(4) Functional Unit Manager: Any person within the Department of Corrections or OCE who reports to either ~~the~~a Director, Deputy Director, an Assistant Director, or an administrator and has responsibility for delivery of program services or coordination of program operations.¶
(3~~5~~) ~~DOC Standard Access: The combination(s) of hardware and software which the Assistant Director for General Services/designee and the Assistant Director for Operations/designee determine to be the standard computer configuration for inmates.¶~~
~~(4) Information Systems Unit (ISU): The unit that is responsible for providing technical or operational support to the DOC Information System or DOC Inmate Network.¶~~
~~(5) Inmate: Any person under~~ Information Security Officer (ISO): The individual within the Department of Corrections who has the responsibility to establish and maintain information security policy, assess threats and vulnerabilities, perform risk and control assessments, oversee the governance of security operations, and establish information security training and awareness programs. The ISO also interfaces with~~e supervision of the Department of Corrections who is not under parole, probation or post-prison supervision status.¶~~
~~(6) Inmate Access: Inmate access to, or use of, computer equipment which is granted because of work,~~ecurity operations to manage implementation details and with auditors to verify compliance to established policies. The ISO is responsible for coordinating program ~~assignment, or authorized by Departme~~requirements throughout the agency with designated points of ~~Corrections rule or policy~~contact and project managers.¶
(~~7~~6) In~~mate Supervisor: Any employee of the Department of Corrections, any OCE employee, or any DOC/OCE contractor that is responsible for supervising an inmate.¶~~
~~(8) 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 Correc~~formation Technology (IT): Any equipment or interconnected system or subsystem of equipment, including computers, ancillary equipment, software, firmware and similar procedures, services and support services, and related resources, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information~~s~~. For purposes of th~~is rule only, Oregon Corrections Enterprises shall not be considered an external organization.¶~~
~~(9) OCE Functional Unit M~~e preceding sentence, equipment is used by an ager~~: Any person within the Oregon Corrections Enterprises who reports to either the Administrator or the Deputy Administrator and has responsibilit~~ncy if the equipment is used by the agency directly ~~for delivery of business services or coordination of business operations.¶~~
~~(10) OCE Standard Access: The combination(s) of hardware and software which the OCE Administrator and the Assistant Director for Operations/designee determine will be accessed by inmates within each correctional institution.¶~~
~~(11) Program Assignment: Any assignment fulfill~~is used by a contractor under a contract with the agency which:¶
(a) requires the use of such equipment; or¶
(b) requires the use, to a significant extent, of such equipment ing the ~~requirement of the inmate's Oregon corrections plan, or ot~~performance of a service or the furnishing of a product.¶
(7) Information Technology Services (ITS): The~~r~~ Department of Corrections ~~approved performance recognition~~

~~program.¶~~
~~(12) Special Access: The combination(s) of hardware and software beyond what is determined to be standard acces~~unit that is responsible for providing technology services and support to the agency, staff, contractors, volunteers, or AICs.
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: 291-086-0030

RULE SUMMARY: Amends rule to add general provisions for AIC access, security, requests, donations, and staff responsibilities; and to update terminology.

CHANGES TO RULE:

291-086-0030
General ¶

(1) ~~These rules (OAR 291-086-0010 through 291-086-0060) establish the approval process and set the standards for inmate access to and use of any information systems equipment; specifically computer hardware and software, peripheral devices, data communications devices, terminals, personal computers, and printers.¶~~
~~(2) Inmates shall only be granted access to computer equipment because of work or program assignment, except for access to resource materials as provided in Department of Corrections rule or policy.¶~~
~~(3) Approval for inmate access to computer equipment is not a privilege or benefit. Any decision to deny or restrict an inmate access to computer equipment may not be appealed by the inmate~~AIC Access to Approved Information Technology: AICs may only be granted access to approved information technology and only for purposes approved by the functional unit manager or designee and ITS in accordance with these rules. Approved purposes may include but are not limited to education programs, Career and Technical Education (CTE) programs, reentry programs, work and program assignments, food services, law library services, general library services, recreation programs, and other approved programs.¶
(2) IT Security Measures: The Department of Corrections shall employ IT security measures to ensure AICs only have access to approved information technology, systems, applications, or websites. These measures may include but not be limited to operating system usage restrictions, firewalls, log aggregation, keystroke logging, or session mirroring.¶
(3) Requests for Purchase, Acquisition, or Implementation of AIC Information Technology: All proposed requests for the purchase, acquisition, or implementation of AIC information technology shall be reviewed by the Information Security Officer (ISO), ITS Technical Services Manager, and the Assistant Director of Operations to ensure all AIC accessible devices and systems are researched and approved as meeting any security protocols established by the DOC ISO and Department of Administrative Services (DAS) Cyber Security Services.¶
(4) Donations: No DOC facility or office shall accept any donated information technology from any individual or organization without the prior written approval of the Assistant Director of Administrative Services and the Assistant Director of Operations.¶
(5) All staff responsible for acquiring information technology for AICs shall follow DOC policies on procurement and contracting. Staff who are requesting new acquisition of, or upgrades to, information technology should familiarize themselves with the aforementioned policies.¶
(6) Staff shall observe all state and federal requirements regarding the handling and sharing of confidential legal work and education records.¶
(7) Staff shall be responsible for the control and security of any media, Wi-Fi, wired connectivity or telephone line used within an area where AICs are allowed to access information technology.
Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

ADOPT: 291-086-0036

RULE SUMMARY: Adopts rule to establish responsibility for the management of approved information technology, and guidelines for service, auditing, and labeling.; and to update terminology.

CHANGES TO RULE:

291-086-0036
Management of Approved Information Technology
(1) The Chief Information Officer (CIO) or designee is responsible for the overall management of information technology authorized for approved use by AICs, which shall include, but is not limited to:¶
(a) Installation and maintenance of information technology systems;¶
(b) Installation and maintenance of information technology software;¶
(c) Installation and configuration of internet connection(s);¶
(d) Implementation of security controls;¶
(e) Securing and maintaining appropriate licenses;¶
(f) Updating information technology systems, software, and security controls, as necessary;¶
(g) Setting up network folders and authorizing access to appropriate internet sites;¶
(h) Blocking access to certain internet sites;¶
(i) Ensuring that AICs cannot use information technology to access any confidential information, Departmental sites or programs, or unapproved external sites or entities;¶
(j) Maintaining a list of authorized internet sites and notifying applicable staff of any changes to the list;¶
(k) Managing AIC user accounts to include expiration dates, size limitations, etc.;¶
(l) Ensuring appropriate staff monitor information technology access by AICs to improve service levels and prevent unauthorized use or access by AICs;¶
(m) Ensuring that any security breaches related to AIC information technology access are reported and appropriately investigated;¶
(n) Overseeing audits of information technology access by AICs; and¶
(o) Providing any necessary technical assistance to staff that are responsible for supervising information technology access by AICs.¶
(2) Service or repair work to be performed on information technology must not be performed in the presence of an AIC unless authorized by the ITS Technical Services Manager or designee.¶
(3) Information technology systems and AIC accounts must be routinely audited no less than once every six months by staff who are familiar with the usage of the system and trained to look for security issues or violations.¶
(4) Audits will be logged and provided to work or program supervisors on a quarterly basis. Audits highlighting or identifying security issues will be provided to the ISO immediately. Work or program supervisors will submit an annual report containing the previous year's audit reports to the ISO and the Assistant Director of Operations.¶
(5) All information technology approved for AIC access will be identified as such with highly visible, conspicuous labeling.
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: 291-086-0040

RULE SUMMARY: Amends rule to update terminology and further define process.

CHANGES TO RULE:

291-086-0040
~~Approval~~ Process for ~~Inmate Access to Computer Equipment~~ Authorizing AIC Access to Approved Information Technology ¶

(1) All requests for ~~inmate computer equipment use shall be approv~~AIC access to information technology must be submitted ~~by~~to the ~~DOC~~ functional unit manager or ~~the OCE functional unit manager~~designee for approval, depending on the area of responsibility, prior to granting access to the ~~inmate~~AIC.¶
(2) The ~~DOC~~ functional unit manager or ~~the OCE functional unit manager may grant standard access. Any request for access that includes hardware or software that is purchased or donated beyond what is determined to be standard access (special access) shall require a recommendation from the functional unit manager requesting the access, a technical review by ISU or OCE for implementation problems, and approval by the Institutions Administrator~~designee may only grant access to approved information technology. Any request for access to information technology that is not approved information technology must be denied.¶
(3) All requests for ~~inmate~~AIC access to ~~computer equipment~~information technology shall be submitted on ~~the Inmate A~~an AIC access to ~~Auto~~information ~~Equipment and Work Assignment R~~technology request form (CD~~-~~1426A). The ~~inmate~~AIC supervisor shall submit the request to the ~~DOC~~ functional unit manager or ~~OCE functional unit manager~~designee for approval. If approved, the ~~inmate~~AIC supervisor and the ~~DOC~~ functional unit manager or ~~OCE functional unit manager~~designee shall sign the request form~~,~~ and forward it to ~~ISU or OCE~~the technical support ~~for implementation. If special access is required, the Institutions Administrator shall approve and sign the request form.¶~~
~~(4) The Assistant Director for General Services/designee and the Assistant Director for Operations/designee will determine specifically what software and hardware combinations constitute DOC standard access.¶~~
~~(5) The OCE Administrator/designee and the Assistant Director for Operations/ designee will determine specifically what software and hardware combinations constitute OCE standard access~~unit responsible for implementation of the requested system (ITS or OCE).¶
(~~6~~4) I~~T~~S~~U~~ or OCE technical support will configure a ~~computer~~ccess as specified in the ~~Inma~~submitted AIC access to ~~Auto~~information ~~Equipment and Work Assignment Request form.¶~~
~~(a) Login accounts will be created for the number of inmates~~technology request form.¶
(a) A domain user account and network storage location will be created for any approved AIC specified ~~i~~on the form.~~¶~~
~~(b) An inmate shared folder(s) on the computer or network hard drive will be created. This folder(s)~~ who does not already have such.¶
(b) The network storage location is the only authorized data storage location ~~on the computer or network~~for AIC use.¶
(~~7~~5) No ~~inmate~~AIC shall be granted access to ~~computer equipment or systems~~information technology which contains data ~~or are connected in any way to the DOC information system network unless the request for access has been reviewed, approved and recommended by either the DOC functional unit manager or the OCE functional unit manager and the Institutions Administrator. The Assistant Director for General Services shall determine final approval for such access~~deemed inappropriate for AIC access by the DOC ITS ISO or is connected in any way to the DOC information system network.¶
(~~8~~6) The ~~inmate~~AIC supervisor shall review the standards for ~~computer~~information technology use listed in OAR 291-086-0050 ~~or 291-085-0060~~ with the ~~inmate~~AIC prior to allowing the ~~inmate to use computer equipment~~AIC to use information technology.¶
(7) The functional unit manager or designee shall maintain a file of all approved requests for AIC access to information technology.¶
(~~9~~8) ~~Inmate~~AIC supervisors shall abide by all ~~the~~ department rules and standards governing ~~inmate~~AIC access to ~~computer equipment. Inmate~~information technology. AIC supervisors are responsible for all work done by ~~inmates on computer equipment~~AICs on information technology and shall:¶
(a) Perform periodic audits of software and data on the equipment to ensure appropriateness;¶
(b) ~~Ensure that regular backups of department data are performed; and~~¶
~~(c) Maintain contingency plans for the accidental or willful destruction of data, software, or hardware.¶~~
~~(10) The DOC functional unit manager or designee or the OCE functional unit manager or designee shall maintain a file of all approved requests for inmate access to computer equipment and proof of licenses for installed software per computer~~Perform routine review of AIC access to information technology request forms no less

than annually to ensure ongoing necessity.¶
(~~11~~9) As appropriate, IT~~SU~~ or OCE technical support will perform random reviews of ~~the~~ DOC or OCE ~~computer equipment~~information technology systems respectively to ensure ~~the~~ configurations conform~~s~~ to the approved configuration o~~n~~f the ~~request form. The DOC or OCE~~system. The functional unit manager may contact IT~~SU~~ or OCE technical support to request an audit of specific ~~computer equipment.¶~~
~~(12~~information technology systems.¶
(10) Suspension or Restriction of AIC's Access to Information Technology: ¶
(a) Any DOC or OCE manager may suspend the authorization for an ~~inmate to use computer equipment if viol~~AIC to access and use information~~s t~~ ~~o this rule~~echnology if rule violations are suspected. ¶
(~~a~~b) The institution assignment office will be notified of the suspension and remove the ~~inmate from the work assignment~~AIC from any assignment related to information technology and place ~~him/her~~the AIC on "Review" status.¶
(~~b~~c) Staff shall r~~emove the computer from the work area or secure it~~strict access to the system in such a manner as to ensure ~~that inmates will not have~~AIC cannot access ~~to~~ it.¶
(~~c~~d) As provided in this rule, the ~~inmate~~AIC supervisor(s) will audit the ~~data~~usage o~~n~~f the ~~compu~~syste~~r~~m and may request IT~~SU~~ or OCE to ~~conduct an investigation of the computer equipment~~investigate the system by sending a formal request to I~~SU~~TS Security or OCE management. DOC requests will be ~~through the ISU Helpdesk~~submitted to the ITS Security Confidential email distribution list. OCE requests will be through OCE ~~technical support~~support services. Findings will be reported to the functional unit manager who signed the ~~original~~investigation request form.¶
(~~d~~e) If rule violations are found to have occurred, appropriate actions will be taken including~~,~~ but not ~~be~~ limited to~~,~~ disciplinary misconduct reports, program failures, and permanent restriction from a~~ny DOC inmate work or program computer system~~ccess to and use of information technology.¶
(~~e~~f) As part of this process, IT~~SU~~ or OCE technical support may recommend to the functional unit manager or designee a course of action to mitigate any problem which arises because of an ~~inmate's use of computer equipment~~AIC's use of information technology.¶
(g) A decision to suspend or otherwise restrict an AIC's access to information technology resulting from a misconduct report or disciplinary order issued under OAR 291-105 (Prohibited Conduct and Processing Disciplinary Actions) is subject to review only as provided in OAR 291-105.¶
(1~~3~~1) Any changes from the original ~~Inmate A~~AIC access to ~~Auto~~information ~~Equipment and Work Assignment R~~technology request form~~,~~ must follow the same approval process as a new request. ~~Changes include hardware requirements, application software additions or deletions, modification to automation request purpose, and adjustments to the number of inmates using the automation equipment~~¶
(12) AIC access to and use of information technology is not guaranteed and may be affected by technological limitations, system updates or failures, hardware malfunctions, facility security necessities, or acts of nature.
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: 291-086-0045

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

CHANGES TO RULE:

291-086-0045
Approval Process for ~~Inmate Computer Operator on a Work Assignment Computer~~ AIC Information Technology User Accounts ¶

(1) Supervisors ~~who need an inmate(s) for a work assignment which involves use of computer equipment~~submitting an AIC access to information technology request form shall submit ~~a~~the request through the institution assignment office. The assignment office will screen the ~~inmate~~AIC(s) for ~~the~~ appropriateness of the assignment ~~and report any ineligibility~~or eligibility of the AIC(s) and report findings to the requestor.¶
(2) Criterion that will exclude an ~~inmate from working on computers~~AIC from using information technology includes~~,~~ but is not limited to~~,~~ computer ~~crime~~-related crime(s), identity theft crime(s), or documented violation of this rule.¶
(3) ~~Inmate~~AICs approved for access to ~~computer equipment must sign the Inmate A~~information technology must sign an AIC access to ~~Auto~~information ~~A~~technology acknowledgement ~~S~~statement (CD~~-~~ 1426B) prior to using ~~the automation equipment.¶~~
~~(4) Inmate~~any information technology system.¶
(4) AICs approved for access to ~~computer equipment~~information technology will need to obtain an ~~inmate password~~AIC domain user account from ITS~~U~~ or OCE.¶
(a) The supervisor shall request a ~~password~~domain user account for the ~~inmate~~AIC by forwarding a copy of the ~~Inmate A~~AIC access to ~~Auto~~information ~~A~~technology acknowledgement ~~S~~statement ~~(CD-1426B)~~ to ITS~~U~~ or OCE.¶
(b) ITS~~U~~ or OCE will ~~issue a password to the inmate.¶~~
~~(c) In the event the inmate shares the password, he/she shall send an Inmate Communication Form to the supervisor. The inmate supervisor shall request ISU or OCE to provide ano~~follow their standard procedures for creating a user account.¶
(c) AIC user accounts will be created using username and password requirements matching current DOC standards, a standardized storage size limit, and an expiration date to not exceed their ~~password~~release date.¶
(d) The ~~inmate~~AIC supervisor shall inform ITS~~U~~ or OCE of any changes in ~~inmate operator(s)~~an AIC's approved access to information technology. ITS~~U~~ or OCE will update the ~~inmate comput~~AIC user acc~~ess~~ount to reflect the change, up to and including deletion of the 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

REPEAL: 291-086-0046

RULE SUMMARY: Repeals rule as no longer needed due to reorganization and other updates to these rules.

CHANGES TO RULE:

~~291-086-0046~~
~~Approval Process for Inmate Computer Operator on a Program Assignment Computer~~
~~(1) Inmate access shall be restricted to those in an approved inmate program assignment. Inmate supervisors will determine inmate eligibility to program assignments requiring access to computers.¶~~
~~(2) The inmate supervisor shall request ISU provide a login account(s) for each program assignment computer. ISU will create the inmate login account(s). The login account will provide access to only the needed program assignment materials.¶~~
~~(3) The inmate supervisor shall inform ISU of any changes in a program assignment that requires access to other computer resources on the computer equipment. ISU will update the inmate login accounts to reflect the change.~~
~~Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075~~
~~Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075~~

REPEAL: 291-086-0047

RULE SUMMARY: Repeals rule as no longer needed due to reorganization and other updates to these rules.

CHANGES TO RULE:

~~291-086-0047~~
~~Approval Process for Inmate Computer Operator on a Resource Computer~~
~~(1) Inmate access to resource computer equipment (e.g., legal library) shall be restricted to services provided by department rule or policy.¶~~
~~(2) The inmate supervisor shall request ISU provide a login account for the resource computer equipment. ISU will issue a login account for the resource computer equipment. The login account will restrict inmate access to only the needed resources.¶~~
~~(3) The inmate supervisor shall inform ISU of any change in resource computer login requirement. ISU will update the inmate computer login to reflect the change.~~
~~Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075~~
~~Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075~~

ADOPT: 291-086-0049

RULE SUMMARY: Adopts rule to establish guidelines governing AIC requests for access to information technology to assist with a disability.

CHANGES TO RULE:

291-086-0049
AIC Process for Requesting Information Technology to Assist With a Disability
(1) To request information technology to assist with a disability, an AIC should contact the institution ADA Coordinator to make an accessibility request. All information technology requested through the accessibility request process are subject to ITS or OCE review and approval.¶
(2) In the event of non-use, improper use, or abuse of information technology described in this rule, an AIC's access to approved information technology may be modified, suspended, or restricted.
Statutory/Other Authority: 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: 179.040, 423.020, 423.030, 423.075

AMEND: 291-086-0050

RULE SUMMARY: Amends rule to update terminology, remove gendered language, and clarify and further define process.

CHANGES TO RULE:

291-086-0050
Standards for Use of ~~Standalone Computer Equipment by Inmate~~Information Technology by AICs ¶

(1) No ~~inmate~~AIC shall be permitted to enter, view, update, or manipulate information ~~on computer equipment~~within information technology systems except as authorized by the ~~DOC~~ functional unit manager or ~~the OCE functional unit manager~~designee and their specific AIC access to information technology request form.¶
(2) Once an ~~inmate~~AIC has been granted access to ~~computer equipment~~an information technology system, the~~/she~~ AIC shall not be allowed to use the ~~equipment~~system without specific assignment by supervising staff. No ~~inmate~~AIC shall create, modify, or change programs or ~~program~~ scripts that will be used on the ~~DOC Information System or DOC Inmate N~~department's AIC network without the approval of the Assistant Director of ~~General Serv~~Operations and the Information Security Office~~s~~r or ~~his/~~their designees.¶
(3) An ~~inmate~~AIC shall be supervised at all times while using ~~computer equipment~~information technology.¶
(4) An ~~inmate~~AIC shall only use ~~computer equipment~~approved information technology which has been approved and authorized in accordance with the ~~department's rule on Inmate Access to Automation (OAR 291-086)~~se rules.¶
(5) An ~~inmate~~AIC shall not repair or modify ~~computer equipment except as part of an authorized Department of Corrections workforce development~~information technology systems except as part of an approved and authorized program.¶
(6) An ~~inmate~~AIC shall not be allowed direct access to printers~~. Printers for inmate~~ or multi-function devices. Printers and multi-function devices for AIC use shall be caged or secured to eliminate direct ~~inmate~~AIC access~~, except as authorized by the DOC functional unit manager or the OCE functional unit manager and Institutions Administrator. All print outs shall~~. All print outs shall be reviewed by staff.¶
(7) An AIC shall not view, gather, or store personal data relating to any person other than themselves, unless authorized by the program they are participating in.¶
(8) An AIC shall not control or possess any computer media except that which has been reviewed ~~by~~, approved, and authorized by supervising staff.¶
(~~7~~9) An ~~inmate~~AIC shall not ~~gather or store personal data relating to staff, contractors or volunteers~~utilize information technology outside of the unit or area for which they are approved.¶
(~~8~~10) An ~~inmate~~AIC shall not ~~view, gather or store personal data relating to members of~~share or divulge their user account password for any reason. When performing routine system checks, the AIC supervisor will have the ~~g~~AIC enter~~al public~~ their password into the system.¶
(~~9~~11) An ~~inmate~~AIC shall not ~~view, gather or store personal data relating to other inmates or offenders, unless authorized by department rule or policy~~be allowed to manage any programs that affect AIC assignments or allocations.¶
(12) No AIC shall create or maintain content that is published to an official department website, OCE website, or external website unless reviewed by staff prior to publishing and as part of an approved and authorized program.¶
(10~~3~~) A~~n inmate~~ICs approved for information technology access shall ~~not~~ have ~~in his/her control or possession any computer media; e.g., diskettes, CDs or tapes except as authorized by supervising staff. An inmate shall not use or take computer equipment to his/her housing area or from his/her immediate work site without approval~~no expectation of privacy or confidentiality when using information technology. DOC shall monitor all aspects of DOC IT systems and such monitoring may occur at any time, without notice, and without the user's permission.¶
(14) No AICs will be present in any room with information technology systems without supervising staff being present.¶
(15) AICs are prohibited from password protecting files.¶
(16) AICs shall not use information technology to conduct or otherwise operate a business without authorization.¶
(17) AICs are prohibited from accessing any wireless network used in the administrative operations of DOC or any wireless network used by individuals, organizations, or other entities outside of DOC.¶
(11~~8~~) A~~n inmate shall not have any unique passwords, except as authorized by ISU or OCE. The password will be created,~~ICs are prohibited from consuming food or beverages when using or around information technology.¶
(19) AICs approved for access are prohibited from using information technology for the following:¶
(a) To violate copyright laws;¶
(b) To harass or threaten anyone;¶

(c) For any illegal activity;¶
(d) To commit any violation of DOC Prohibited Conduct;¶
(e) To access pornography;¶
(f) To access any materials that would not be allowed to be rec~~orded, and issued by ISU or OCE and will not be changed by the inmate.¶~~
~~(12) An inmate shall not be allowed to manage any programs that affect inmate assignments or allocations.¶~~
~~(13) Without the approval of the Director or designee, no inmate shall create or maintain Internet or website content that is published to an official department Internet/web site~~eived via the mail as set out in DOC rule 291-131 Mail (AIC);¶
(g) To upload any program or introduce any virus into any information technology system;¶
(h) To impersonate any other person, falsely represent themself, or make any other false statement in connection with information technology use;¶
(i) To intentionally or negligently destroy, damage, or cause a malfunction of any information technology system;¶
(j) To contact anyone with whom they have a no contact order or who is a victim of a crime committed by them;¶
(k) To contact anyone on behalf of another AIC for any reason; or¶
(l) To allow another AIC access to the individual's user account, user ID, password, or storage locations.¶
(20) AICs who violate any of these aforementioned prohibitions are subject to any or all of the following: termination of approval for information technology access, disciplinary or other administrative action, or criminal prosecution.
Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075

REPEAL: 291-086-0060

RULE SUMMARY: Repeals rule as no longer needed due to reorganization and other updates to these rules.

CHANGES TO RULE:

~~291-086-0060~~
~~Standards for Use of Network Computer Equipment by Inmates~~
~~(1) No inmate shall be permitted to store any data on the computer or network hard drive except as authorized by the inmate supervisor. A folder(s) will be created by ISU or OCE and shall be the only authorized data storage location.¶~~
~~(2) Once an inmate has been granted access to computer equipment, he/she shall not be allowed to use the computer equipment without specific assignment by supervising staff. No inmate shall create, modify or change programs or program scripts that will be used on the DOC Information System or DOC Inmate network without the approval of the Assistant Director of General Services or his/her designee.¶~~
~~(3) An inmate shall be supervised while using computer equipment.¶~~
~~(4) An inmate shall only use computer equipment which has been authorized in accordance with the department's rule on Inmate Access to Automation (OAR 291-086).¶~~
~~(5) An inmate shall not repair or modify network computer equipment except as part of an authorized Department of Corrections workforce development program.¶~~
~~(6) An inmate shall not be allowed direct access to printers. Printers for inmate use shall be caged or secured to eliminate direct inmate access, except as authorized by the DOC functional unit manager or the OCE functional unit manager and Institutions Administrator or his/her designee. All print outs shall be reviewed by staff.¶~~
~~(7) An inmate shall not use the network for electronic communications with other inmates.¶~~
~~(8) An inmate shall not gather or store personal data relating to staff, contractors or volunteers.¶~~
~~(9) An inmate shall not view, gather or store personal data relating to members of the general public.¶~~
~~(10) An inmate shall not view, gather or store personal data relating to other inmates or offenders except as authorized by department rule or policy.¶~~
~~(11) An inmate shall not have in his/her control or possession any computer media, e.g., diskettes, CDs or tapes except as authorized by supervising staff. An inmate shall not use or take computer equipment to his/her housing area or from his/her immediate work site without approval.¶~~
~~(12) An inmate shall not have any unique passwords, except as authorized by ISU. The password will be created, recorded and issued by ISU or OCE and will not be changed by the inmate.¶~~
~~(13) An inmate shall not be allowed to manage any programs that affect inmate assignments or allocations.¶~~
~~(14) Without the approval of the Director or designee, no inmate shall create or maintain Internet or website content that is published to an official department Internet/web site.~~
~~Statutory/Other Authority: ORS 179.040, 423.020, 423.030, 423.075~~
~~Statutes/Other Implemented: ORS 179.040, 423.020, 423.030, 423.075~~

ADOPT: 291-086-0070

RULE SUMMARY: Adopts rule to establish guidelines for AICs to request a review when their access to information technology has been restricted.

CHANGES TO RULE:

291-086-0070
Review of Access Restrictions
Upon being notified of the department's decision to restrict an AIC's access to information technology, the AIC may request review of the decision through:¶
(1) The administrative hearings process as governed by OAR 291-105, if a misconduct report has been submitted for the action;¶
(2) The grievance review system as governed by OAR 291-109, if no misconduct report has been submitted for the action; or¶
(3) The ADA grievance process as governed by OAR 291-111, if the AIC's access restriction is for information technology described in OAR 291-086-0049.
Statutory/Other Authority: 179.040, 423.020, 423.030, 423.075
Statutes/Other Implemented: 179.040, 423.020, 423.030, 423.075

ADOPT: 291-086-0071

RULE SUMMARY: Adopts rule to establish guidelines for the removal of restrictions to access information technology for AICs.

CHANGES TO RULE:

291-086-0071
Removal of Access Restriction
(1) An AIC may request that their restriction from access to information technology be removed after one year from the restriction date.¶
(a) To request removal of a restriction from access to information technology an AIC must send an AIC communication form requesting removal of the access restriction, together with any supporting documentation, to the designated committee at the facility where the AIC is currently housed. Documentation submitted as part of this review process will not be returned to the AIC. The request should support that the AIC has demonstrated significant positive behavior change and no longer poses a threat to the security of the facility, the department, or the community through access to information technology.¶
(b) The designated committee may gather information pertinent to the restriction review. The review will include a recommendation from ITS.¶
(c) The designated committee shall complete its review within 30 days after receiving the AIC's request for removal of the access restriction. If the review takes longer than 30 days, the reason for the delay will be documented with the resulting recommendation. The committee will forward their recommendation to the DOC Operations Technology Liaison.¶
(2) The DOC Operations Technology Liaison or designee, shall review and track the recommendation provided by the designated committee. The DOC Operations Technology Liaison will forward the recommendation to the Institutions Administrators or their designees for decision. The decision will ordinarily be issued within 30 days of receipt. If the review takes longer than 30 days, the reason for the delay will be documented.¶
(3) The Institutions Administrators or their designees shall notify the AIC of the decision in writing. The decision shall be final and is not subject to further review for a period of one year from the date of the decision.¶
(4) Requests for removal of restrictions from access to information technology described in OAR 291-086-0049 must be submitted and processed through the ADA accessibility request process as governed by OAR 291-111.¶
(5) Notwithstanding paragraphs (1) through (4) of this rule, an AIC actively engaged in a reentry program that requires the use of information technology may, by approved exception, continue to participate in the program and utilize information technology deemed necessary by the program administrator under the following conditions:¶
(a) The reentry program administrator must document and maintain written approval for the exception; and¶
(b) The AIC must utilize the information technology only for the specified reentry programs in the exception approval; and¶
(c) The utilization of the information technology must be provided in a direct supervision environment.
Statutory/Other Authority: 179.040, 423.020
Statutes/Other Implemented: 179.040, 423.020