OFFICE OF THE SECRETARY OF STATE
TOBIAS READ
SECRETARY OF STATE

MICHAEL KAPLAN
DEPUTY SECRETARY OF STATE

ARCHIVES DIVISION
STEPHANIE CLARK
DIRECTOR

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

PERMANENT ADMINISTRATIVE ORDER

DAS 2-2026

CHAPTER 125

DEPARTMENT OF ADMINISTRATIVE SERVICES

FILED: 04/28/2026 9:12 AM

ARCHIVES DIVISION SECRETARY OF STATE & LEGISLATIVE COUNSEL

FILING CAPTION: Renumber Chapter 125 Division 600 and 800 to Office of the State CIO Chapter 128.

EFFECTIVE DATE: 05/01/2026

AGENCY APPROVED DATE: 04/23/2026

CONTACT:
Janet Chambers
971-720-0824
janet.chambers@das.oregon.gov
155 Cottage Street NE
Salem, OR 97301

Filed By:
Janet Chambers
Rules Coordinator

RULES:
125-600-0005, 125-600-7550, 125-800-0005, 125-800-0010, 125-800-0020

RENUMBER: 125-600-0005 to 128-050-0005

RULE SUMMARY: Renumber rule to Office of the State CIO Chapter 128 Division 50.

CHANGES TO RULE:

125~~-600~~8-050-0005
Guidelines for Use of Electronic Signatures by State Agencies ¶

(1) The purpose of this rule is to implement the electronic signature provisions of the Uniform Electronic Signatures Act (UETA). The rule is not intended to apply to the other provisions of the act.¶
(2) This rule applies prospectively to new software applications with electronic transactions requiring signatures that are implemented after the effective date of this rule.¶
(3) Agencies shall follow the Information Resources Management Division policy which adopts the federal E-authentication process. The IRMD policy requires that agencies using electronic signatures:¶
(a) Determine the level of assurance the agency needs that the party signing an electronic transaction is authentic.¶
(b) Use only those tools and software applications approved by NIST and the Department of Administrative Services, Information Resources Management Services Division to mitigate the risks identified and provide the

level of authentication needed.¶
(4) Agencies may request an exemption from these rules from the Department of Administrative Services.
Statutory/Other Authority: ORS 184.305, 291.038, 84, 84.049, 84.052, 84.055, 84.064
Statutes/Other Implemented: Portions of 2001 HB 2112

RENUMBER: 125-600-7550 to 128-040-0005

RULE SUMMARY: Renumber rule to Office of the State CIO Chapter 128 Division 40.

CHANGES TO RULE:

12~~5-600-7550~~8-040-0005
Enterprise Geographic Information System (GIS) Software Standard ¶

(1) Purpose. The purpose of this rule is to establish a common, enterprise GIS Software standard to promote the creation, use and exchange of inter-related and standards-based geographic data and geospatial business intelligence within and between state agencies. The objective of this standard is to provide a common geospatial software and data framework underpinning all future computer applications containing geospatial components thus increasing the value and use of those applications as state information technology assets. The GIS Software standard will also allow the State of Oregon the opportunity to leverage the buying power of the broadest possible user base. The GIS Software standard is anticipated to enable the most integrated, economic and efficient acquisition, installation and use of GIS across Oregon state government. These outcomes will be made possible through the:¶
(a) Current installed base of GIS software and trained expertise within state agencies.¶
(b) General technical benefits associated with the use of standardized software, including but not limited to:¶
(A) Simplified software and application infrastructure configurations.¶
(B) Ease of software installations and upgrades.¶
(C) Simplified application connectivity, security and data distribution architectures.¶
(D) The capacity for simultaneous multi-user editing, dataset versioning, and history retention.¶
(E) The ability to utilize existing geospatial business intelligence to ensure data integrity and consistency via the establishment of topology rules, data attribute domain rules, and data validation rules.¶
(c) Enterprise-oriented data and application accessibility offered by the use of common GIS software deployed across state agencies.¶
(d) Enhanced functionality and interoperability of related software components within a suite of software applications including the reduction of costly data translations between diverse software products and the ability to leverage data modeling and processing efforts for reuse between agencies.¶
(e) Ease of sharing geospatial data among agencies and with the public based on a common GIS software infrastructure.¶
(2) Definitions. For the purposes of this rule:¶
(a) "GIS" means geographic information systems which comprise the hardware, software, network, data, and human resources involved in creating, maintaining, managing, and distributing data, information, and knowledge about spatial objects and their relative positions.¶
(b) "GIS Software" means computer-language coding created specifically to facilitate the creation, management, distribution, accessibility, and promulgation of Spatial Data. For the purposes of this rule, "GIS Software" does not mean computer-language coding used for the purposes of computer aided design (CAD), simple address list management or similar business processes unless the purpose is to establish inter-agency Spatial Data.¶
(c) "Spatial Data" means digital information that identifies the geographic location of features and boundaries that are usually stored as coordinates and topology that can be mapped or used for comparative spatial analysis.¶
(d) "State Agency" or "Agency" means every state officer, board, commission, department, institution, branch or agency of the state government, whose costs are paid wholly or in part from funds held in the State Treasury, except:¶
(A) The Legislative Assembly, the courts and their officers and committees;¶
(B) The Public Defense Services Commission;¶
(C) The Secretary of State and the State Treasurer in the performance of the duties of their constitutional offices;¶
(D) The State Board of Higher Education or any state institution of higher education within the Oregon University System; and¶
(E) The State Lottery.¶
(3) Standard. To achieve the purposes described in section (1) of this rule the standard for GIS Software for Oregon state agencies is the scalable suite of Environmental Systems Research Institute, Inc (ESRI) software applications:¶
(a) Deployed at the desktop, server, or web interface levels and designed to enable the creation, manipulation, management, storage and distribution of digital maps, digital spatial objects and any associated spatial tabular databases; or,¶
(b) To manage shared spatially-referenced information.¶
(4)(a) GIS Software Inventory. All state agencies shall inventory and report use of all GIS Software in the format and

at the time established by DAS Enterprise Information Strategy and Policy Division (EISPD). Upon conclusion of the inventory the exception process described in subsection (5) of this rule becomes effective.¶
(b) Continued use of existing, installed, non-standard GIS Software declared in inventory; assumed exception. Agencies currently using non-standard GIS Software described by the agency in the inventory required by subsection (a) of this section will be granted a written exception to the enterprise GIS Software standard until such time as any of the conditions described in section (5)(d) of this rule occur.¶
(5)(a) Exception. Notwithstanding the enterprise GIS Software standard established in subsection (3) of this rule, the State Chief Information Officer (CIO) or their designee may grant a written exception to an agency to the GIS Software standard.¶
(b) Considerations for evaluating an agency exception request. Considerations to be weighed by the State CIO or their designee in evaluating an agency request for an exception to the GIS software standard include, but are not limited to:¶
(A) Agency business rationale for use of non-standard GIS software;¶
(B) The degree to which the requested non-standard use of GIS software would materially inhibit the state from ensuring that its information resources fit together in a statewide system capable of providing ready access to and sharing of information, computing or telecommunication resources;¶
(C) The degree to which the requested non-standard use of GIS software would interfere with the state's goal of acquiring and using enterprise information technology resources in the most integrated, interoperable, efficient and economical manner possible; and¶
(D) Other factors deemed to be relevant to consider by the State Chief Information Officer (CIO).¶
(c) Agency Exception Request. An agency may be granted an exception to the GIS Software standard by submitting a written exception request to DAS EISPD. An agency exception request must address each of the considerations described in subsection (b) of this section and contain the facts base necessary to justify agency conclusions.¶
(d) Conditions requiring agency to submit an exception request. An agency must submit a written agency exception request to DAS EISPD when the any of the following conditions arise:¶
(A) Use of excepted, non-standard GIS Software evolves over time. Any agency using excepted, non-standard GIS Software must submit a request to continue that exception whenever agency's use of the non-standard GIS Software is anticipated to change. Changes include, but are not limited to:¶
(i) An expansion of the number of software licenses used within the agency.¶
(ii) Changing the license management system from desktop-oriented to network-oriented use.¶
(iii) Changing the software use model from a desktop to a client-server orientation.¶
(iv) Supplementing the existing GIS Software use with a web-based application for functionality, data creation, data sharing, or map product distribution.¶
(B) Initial acquisition of non-standard GIS Software. Before initial acquisition of non-standard GIS Software an agency must request an exception to the GIS Software standard.¶
(C) Non-standard GIS Software used for documented research or instructional purposes. Before initial or expanded use of non-standard GIS Software for research or instructional purposes an agency must request an exception to the GIS Software standard. A single exception request from an agency should be sufficient to cover all research and instruction conducted by any division, unit, or individual of that agency.¶
(e) Emergency exception. Notwithstanding the exception request process described in subsections (c) and (d) of this section, the State CIO may waive some or all of the requirements for written submission of an agency exception request when immediate action is required to address an agency's emergency need to use non-standard GIS Software.¶
(f) Reconsideration. An agency may request reconsideration of a denial of a GIS Software standard exception request by submitting a subsequent request in writing to the State CIO containing additional supporting information that was not included in the original exception request.¶
(6) Biennial Review. At least once every two years the State CIO must issue a written report to the Oregon Geographic Information Council regarding the efficacy of the GIS Software standard and its accomplishment of the purposes described in subsection (1) of this rule.
Statutory/Other Authority: ORS 291.038
Statutes/Other Implemented: ORS 291.038

RENUMBER: 125-800-0005 to 128-030-0005

RULE SUMMARY: Renumber rule to Office of the State CIO Chapter 128 Division 30.

CHANGES TO RULE:

12~~5-80~~8-030-0005
Purpose, Application, and Authority ¶

These rules are adopted under 2005 Oregon Laws Chapter 739. These rules set forth the policies for state government-wide information security.
Statutory/Other Authority: ORS 182.122, 291.038
Statutes/Other Implemented: ORS 182.122

RENUMBER: 125-800-0010 to 128-030-0010

RULE SUMMARY: Renumber rule to Office of the State CIO Chapter 128 Division 30.

CHANGES TO RULE:

12~~5-80~~8-03~~0~~0-0010
Definitions ¶

(1) "Incident" means any material adverse event that impairs the confidentiality, integrity or availability of information resources.¶
(2) "Information Resources" means all categories of automated or non-automated systems and data, including but not limited to, records, files, and databases, information technology equipment, facilities, and software owned or leased by the state.¶
(3) "Material adverse event" means an adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.¶
(4) "Ordinary Public Access" means unauthenticated access to systems or online resources intentionally provided for public use, such as an agency's public web site.¶
(5) "Publicly addressable interfaces" means any network device or software application using Internet protocols that can be accessed using addresses that are routable over the public Internet infrastructure, including the state's backbone network.¶
(6) "Privately addressed interfaces" means any network device or software application using Internet protocols accessed using addresses that are not routable over the public Internet infrastructure, including the state's backbone network.¶
(7) "State Information Security Plan" means a compilation of documents including, but not limited to, statutes, administrative rules, policies, and plans, prescribing the information security practices of the State of Oregon.¶
(8) "Security Assessment" means any organized method of determining the risk or vulnerability including, but not limited to: risk assessment; vulnerability assessment; security penetration test, and security audits and reviews.¶
(9) "State Shared Computing and Network Infrastructure" means all network and information assets under the direct control or maintained by the Executive Department.
Statutory/Other Authority: ORS 184.305; 182.122
Statutes/Other Implemented: 2005 Oregon Laws Chapter 739

RENUMBER: 125-800-0020 to 128-030-0020

RULE SUMMARY: Renumber rule to Office of the State CIO Chapter 128 Division 30.

CHANGES TO RULE:

12~~5-80~~8-030-0020
State Information Security ¶

(1) Duties:¶
(a) Department of Administrative Services (Department): The Department shall serve as the primary point of accountability and coordination for information security in state government except for elected offices as identified in section 4, Elected Offices Exception. The Department, in collaboration with state agencies, shall routinely take necessary actions, proactive and reactive, to protect and verify protection of the state's shared computing and network infrastructure including, but not limited to: active scanning and monitoring; intrusion prevention and detection; scheduled and unscheduled security reviews and compliance audits; protection, containment and mitigation actions taken to address threats, vulnerabilities, and security problems; termination or filtering of connections to mitigate problematic network traffic or unauthorized access; quarantine of infected systems to allow for the forensic identification and analysis of system threats; and the application of other steps and practices as may be required.¶
(A) Leadership. The Department shall provide central leadership for state government-wide information security including, but not limited to: centrally directing and coordinating all enterprise information security activities; determining security risks to the state's Information assets and collaboratively working with state agencies in taking those actions required to mitigate unacceptable risks; collaboratively work with state agencies to determine appropriate state and agency security activities to maintain appropriate levels of security preparedness and competency; reducing the cost of providing security by implementing an enterprise approach; detecting and eliminating unnecessary duplication of efforts and obstacles to forward progress in information security; creating the processes and process linkages necessary to maintain a fully functional state government security capability; and creating and maintaining the tools and practices necessary to manage the host of simultaneous and interoperable activities that comprise information security.¶
(B) Planning. The Department, in collaboration with state agencies, shall direct information security planning including, but not limited to: determining strategic security objectives and associated performance measures; analyzing and evaluating state, agency and trusted partner security practices; proposing and subsequently prescribing solutions for information security challenges; establishing a process to determine, prioritize and schedule security enhancements on a state government-wide basis; ensuring through validation that information security is an essential part of state and agency business planning and operations; determining essential state information security roles and responsibilities; and identifying opportunities for security master contracting and other procurement efficiencies. The Department may plan, manage and undertake enterprise-level information security projects and initiatives.¶
(C) Policy. The Department, in collaboration with state agencies, shall develop, recommend, implement and maintain the full spectrum of administrative rules, policies, architecture, standards, guidelines, and procedures necessary to create and maintain an appropriate state government-wide information security competency.¶
(D) Coordination. The Department shall coordinate the security activities of state government including, but not limited to: providing the security communications, coordination, planning and development hub for state government; establishing collaborative partnerships with local and regional governments and the Federal government in the realm of security planning and implementation; and enterprise coordination of all information security-related activities and initiatives across state government.¶
(E) Security Assessments. The Department shall work collaboratively with state agencies to conduct information security assessments and testing within Oregon state government including, but not limited to: determining when it is appropriate to outsource security testing of state or agency Information assets; coordinating security assessments and tests; establishing standards for the timing and nature of agency information security assessments and tests including, but not limited to internal and external, third-party assessments; provide oversight for agency vulnerability and risk mitigation planning and actions; and ensuring the dissemination of any security assessment and test report data is restricted to only those who, in the judgment of the State Chief Information Security Officer, Agency Director, and/or appropriate state agency staff, have a business need for such information. The Department shall determine qualifications for vendors contracted to perform security assessments.¶
(F) Incident Response. The Department shall create a state incident response capability including, but not limited to: appointing a standing, multi-agency State Incident Response Team (SIRT) as described in section (2) of this rule;

ensuring the SIRT, in collaboration with state agencies, prescribes and takes those actions necessary to immediately assemble and deploy the coordinated expertise, tools, communications infrastructure, methodologies and controls required to prevent or mitigate damage caused by an Incident. SIRT will perform a structured investigation into the nature and cause of an Incident; document evidence of computer crime, misuse or Incident; employ forensic techniques and controls; evaluate Incidents for improvement of information security; perform any duties required to appropriately defend against an Incident and subsequently prosecute the perpetrator; and cooperate with law enforcement and other authorities.¶

(G) System Management. The Department, in collaboration with state agencies, shall provide policies, standards and consultation on systems management associated with information security including, but not limited to management of: firewalls; routers; intrusion detection and protection mechanisms; identity and access management; patch/configuration management; digital certificates; secure transmission and access controls (encryption); wireless devices; change controls, and automated system log aggregation and monitoring.¶

(H) Security Awareness and Training. The Department will provide the communications practices and tools necessary to form and maintain a viable information security community of practice across Oregon state government including, but not limited to: creation and maintenance of an information security knowledge and document repository; creation and maintenance of a enterprise level user awareness program, and participation with state and national stakeholder groups; provide the training or training curriculum required to: inform managers, users and technologists on the policies and practices of state information security; work with agencies to ensure all who have access to information assets are provided training on their security-related responsibilities and the specific security-related actions they are expected to take; and identifying, conducting or arranging appropriate security certification for key state and agency staff.¶

(I) Reporting. The Department shall continually track and share relevant enterprise security information including, but not limited to: creation and dissemination of standardized reports demonstrating the status and progress of information security efforts across state government. Keep state executive management and the Legislature appraised of the state's information security posture.¶

(J) Performance Management. The Department shall identify, track, analyze, adjust and report information security performance measurement and management to the Legislature, state executive management.¶

(K) Compliance and Oversight. The Department shall require and enforce compliance with information security practices including, but not limited to: performing or directing compliance reviews to ensure agencies are taking appropriate information security actions and adhering to laws, rules, policies, architecture, standards, procedures and guidelines; routinely inventory and evaluate the information security capabilities of the agencies of state government; prescribing a standardized approach for responding to audit and security assessment issues; and taking appropriate action when there is a failure to adhere to information security practices.¶

(L) Financial Management. The Department shall develop budgets and manage the finances for enterprise security projects and initiatives.¶

(M) Procurement. The Department shall manage procurements for the enterprise information security program including, but not limited to: procurement of hardware, software and expertise; approving enterprise security-related procurements; and issuing and managing enterprise-level, information security program contracts; ensuring contract language regarding information security is properly addressed in contracts.¶

(N) Evaluation. The Department shall evaluate and report the risk, feasibility, effectiveness and cost implications of potential enterprise information security issues and provide recommendations for mitigation.¶

(O) State Chief Information Security Officer. The Department will designate a State Chief Information Security Officer to manage and promote information security across the agencies of state government.¶

(b) Agency Responsibilities. The chief executive of each agency is accountable for their agency's information security. Each agency head must: provide active leadership for information security practices within the agency and be responsible for agency security practices; designate an agency security liaison to participate in the collaborative development and implementation of the state security plan, and ensure agency compliance with this rule and the state information security plan; support, cooperate with and participate in the state information security program; report security-related information including, but not limited to, incident reporting, security status reporting, security-related financial reporting, and security audit or risk mitigation action. The agency head may delegate his/her authority for information security to an agency Information Security Officer (ISO), although the overall responsibility for agency information system remains with the agency head.¶

(c) Approval of Agency Security Plans. The Department, in collaboration with state agencies, shall establish standards for agency information assets security plans. Should an agency security plan contradict or contravene, or fail to meet minimum standards established by the state information systems security plan, the Department shall have the right to return the plan to the agency for revision and may decline to certify such plans until the plan has been modified to satisfy the overarching objective of protecting the state's information assets.¶

(d) Security Assessment. The Department shall notify an agency of any negative outcome of any security assessment. If, as a result of a security assessment, the Department determines that there are severe

vulnerabilities, the agency must take appropriate actions in a timely fashion to mitigate identified vulnerabilities. Additionally, the agency shall draft and implement a Security Assessment mitigation plan, subject to the Department's approval, to mitigate the risks identified in the security assessment. The Department shall ensure that the vulnerabilities described in the assessment are mitigated following the approved plan. The Department, in collaboration with the agency, may take any action prudently required to protect the states information assets from unacceptable risks. For the purposes of this rule, risks or vulnerabilities identified by a security assessment, test, or in some other way, may constitute an incident requiring an incident response. The Department shall determine if a risk or vulnerability constitutes an incident.¶

(e) Interagency Collaboration. The Department will work with other governmental jurisdictions within the State of Oregon including, but not limited to all state, local and regional governmental entities contingent upon their written request and an agreement for appropriate cost sharing. The objective of such interaction is development of a cost-effective, common approach resulting in optimization of limited resources and enhanced strategic capabilities.¶

(2) State Incident Response Team:¶

(a) Authority: The State Incident Response Team (SIRT) shall be advised by and collaborate with the State Chief Information Officer, the state Chief Information Security Officer, and appropriate advisory bodies. Each state agency is responsible for creating and implementing an agency-level incident response capability.¶

(b) SIRT Membership: The SIRT is appointed by the Department and is, at a minimum, comprised of: representatives from the Department, Office of Emergency Management (OEM) and Oregon State Police (OSP); agency information security experts; and resources dedicated to incident communications. The members of the SIRT will work collaboratively to develop procedures, rules of engagement, and resource commitments to the SIRT.¶

(c) SIRT Agency Duties: Each agency shall report incidents to the SIRT as prescribed in applicable rules, policies, and procedures. Agencies are required to report incidents, cooperate with and support SIRT activities, and adhere to SIRT policies and procedures.¶

(3)(a) Applicability to Oregon University System: Oregon University System computers, hardware, software, storage media, networks directly connected to the state's computing and network infrastructure, and not exempted by the provisions of 2005 Oregon Laws Chapter 739, are subject to these rules. The Department, in conjunction with Oregon University System, shall determine when such connection has occurred.¶

(b) Applicability to Oregon Lottery: These rules shall apply only to Oregon Lottery computer systems and network devices directly connected to the state's backbone network using publicly addressable interfaces. The Department, in conjunction with the Oregon Lottery, shall determine when such connection has occurred. Subject to constitutional and statutory limitations, the Oregon Lottery will notify the Department in the event of any incident adversely affecting Lottery gaming systems and networks that could impact the state's shared computing and network infrastructure.¶

(4) Elected Offices Exception: The Department shall establish, in collaboration with Elected Officers, criteria to determine compatibility between the information security plans adopted by the Secretary of State, the State Treasurer and the Attorney General (elected officers) and the state information security plan and associated standards, policies and procedures. If a joint information security plan and associated operational standards and policies cannot be agreed upon by the Department and the elected officers, or if the Department determines the information security plans adopted by the elected officers are not compatible with the state information security plan and associated standards, policies and procedures, the Department will continue to work with the elected office agencies to resolve outstanding issues.

Statutory/Other Authority: ORS 182.122, 291.038

Statutes/Other Implemented: ORS 182.122