CYBER AND INFORMATION SECURITY

NUMBER: 107-004-052_PR

EFFECTIVE DATE: October 1, 2026

DIVISION: Enterprise Information Services (State CIO)

POLICY OWNER: Cyber Security Services

INTERNAL/STATEWIDE: Statewide

LAST REVIEWED DATE: July 28, 2026

SUPERSEDES: Procedure #107-004-052_PR (2/17/2026)

REFERENCE/AUTHORITY:

- ORS 276A.300, 276A.303, 276A.306, 276A.323, 276A.326, 276A.329, 276A.332, 276A.335
- OAR 128-30
- Cyber and Information Security policy 107-004-052

APPROVED SIGNATURE:

Terrence Woods, State Chief Information Officer

Statement

This procedure describes Enterprise Information Services (EIS) and agency responsibilities and actions that must be followed to comply with Statewide Policy 107-004-052, Cyber and Information Security.

Applicability

Refer to Statewide Policy 107-004-052, Cyber and Information Security, for applicability of this procedure.

Exhibits

- Cyber Security Services (CSS) Assessment Schedule
- Attachment A: CSS assessment findings and recommendations template
- Attachment B: Plan of Action and Milestones template
- Attachment C: Use of offshore or foreign computing services disclosure data elements

Definitions

Refer to Statewide Policy 107-004-052, Cyber and Information Security, for definitions.

Procedure

ASSESSMENTS

RESPONSIBILITY	STEP	ACTION
Cyber Security Services (CSS)	1	Biennially, publish the CSS Assessment Schedule for two calendar years.
CSS	2	Send assessment engagement letter to agency head and agency IT leader for agency assessments in the upcoming quarter.
Agency head and agency IT leader	3	Attend CSS assessment engagement kickoff meeting with CSS.
CSS	4	Conduct assessment of agency security program.
Agency	5	Participate in CSS assessment of agency security program.
Agency head and agency IT leader	6	Attend CSS assessment exit briefing where CSS will deliver and discuss findings and recommendations with the agency.
CSS	7	Deliver final report to agency head and agency IT leader. (Attachment A)
Agency	8	Document plans of actions and milestones (POAM) and review at least monthly. Quarterly, deliver updated status of identifying and implementing remediations of findings and recommendations for outstanding critical and severe findings. Required POAM elements are defined in Attachment B. Note: CSS may meet with the agency quarterly or as needed to provide consultation for remediation of findings.

ANNUAL TRAINING

RESPONSIBILITY	STEP	ACTION
CSS	1	Update and upload annual cybersecurity training in Workday.
Agency	2	Coordinate with CSS for scheduling training for users.
Chief Human Resource Office and agencies as applicable	3	Schedule training in Workday for all users.
Users	4	Complete annual cybersecurity training by December 31 of each year.

OFFSHORE AND FOREIGN SERVICES

RESPONSIBILITY	STEP	ACTION
Agency	1	Identify current use (as of the effective date of statewide policy 107-004-052) of offshore or foreign computing services.
Agency	2	Provide the information detailed in Attachment C (Use of offshore or foreign computing services disclosure data elements) by submitting to this form.
CSS	3	Review request and make recommendations to State Chief Information Officer.
State CIO or delegated EIS authority	4	Make decision on request.
CSS	5	Respond to agency submission with decision. Decision to approve offshore or foreign computing services may be accompanied by conditions for risk mitigating controls. Decision to disapprove offshore or foreign computing services may be accompanied by expectations for discontinuing offshore or foreign computing services.
Agency	6	Return decision communication with signature acknowledgement by responsible role.

Attachment A: CSS assessment findings and recommendations template

Findings and Recommendations

Finding 1:

Finding Title	Finding Severity

FINDING TITLE	
CIS v8.0 Control	
CIS v8.0 Safeguard	
Artifact(s)	
References	

Finding Detail: Content.

Impact: Content.

Recommendation: Content.

Finding Title	Finding Severity

FINDING TITLE	
CIS v8.0 Control	
CIS v8.0 Safeguard	
Artifact(s)	
References	

Finding Detail: Content.

Impact: Content.

Recommendation: Content.

Attachment B: Plan of Action and Milestones (POAM) template

Plan Element	Plan Element Description	Input by	Input Example
POAM ID	Unique identifier for each POAM item	Agency	AGCY-0101
Safeguard	Applicable control	EIS	01.01
Finding	Brief description of finding	EIS	Agency's consolidated asset inventory contained 2000 deployed items with nearly all expected attributes enumerated. Comparison of Defender and Tenable data with inventory found 350 assets not listed by agency.
Recommended remediation	Proposed remediation action	EIS	Agency should leverage its existing hardware asset management tools to develop and maintain an authoritative inventory of all authorized devices with the potential to receive, store, or process data. The inventory should include end-use devices (including mobile devices), network devices that the organization manages, IoT devices that the organization manages, and servers. For each device, the inventory should document the network address (if static), hardware (MAC) address, machine name, data asset owner, department, and whether the asset has been approved to connect to the network. The inventory should be reviewed for accuracy and updated, at a minimum, bi-annually. Once agency has documented its authorized hardware asset inventory, it should periodically compare output from its asset inventory tools to its authorized hardware asset inventory to review for unauthorized devices.
Criticality	Assigned criticality	EIS	Critical
Assessed score	Safeguard score at the time of assessment	EIS	59.6%
Issue Date	Date finding was issued	EIS	12/31/2024
Recommended remediation date	Calculated based on criticality	EIS	1/30/2025
Agency internal point of contact	Agency personnel assigned to POAM	Agency	Butch Cassidy
Remediation Plan	Overall plan to remediate deficiency	Agency	Create asset inventory

Plan Element	Plan Element Description	Input by	Input Example
Planned milestones	Planned milestones with project completion dates	Agency	(01) 2025-01-10: Extract full inventory of all systems. (COMPLETE) (02) 2025-01-15: Evaluate assets for approval. (COMPLETE) (03) 2025-01-31: Develop procedure to update inventory. (COMPLETE)
Internal comments	Internal agency comments	Agency	Working with BSA and ASCIO-supplied template.
Dependency	Description of any dependencies	Agency	
Support documents	List any supporting documents	Agency	AssetInventory.xlsx
Date closed	Date remediation actions completed	Agency	1/31/2025

Attachment C: Use of offshore or foreign computing services disclosure data elements

Agency Information
Agency
Submitted by
Submitter Email
Submitter Phone Number
Agency Business Owner
Agency Business Owner Email
Agency Business Owner Phone Number
Application/Software Details
Is this a new, renewing, or existing service/application?
Application Name
Version Number
Hosting Architecture: on-premises (state/agency hosted), cloud – SaaS, cloud – PaaS, Cloud – IaaS, hybrid (on-prem + cloud), vendor or contractor hosted (containerized/serverless), other
Vendor and Contract Information
Contracted Vendor Name
Contract Start Date
Contract End Date
Renewal Frequency (i.e., 6 months, 2 years, etc.)
Data Handling and Sensitivity
Highest data classification level (Refer to the Information Asset Classification Policy for additional information https://www.oregon.gov/das/Policies/107-004-050.pdf): level 1 – published, level 2 – limited, level 3 – restricted, level 4 - critical
What regulated data exists in the environment? (HIPAA, FIT, CJIS, PCI, FERPA, not applicable, other)
Offshore Usage Details
Offshore Country Locations (list all offshore countries)
Does data currently reside outside the United States, or is it anticipated that it will reside outside the United States as part of future offshore services?
Does offshore staff access any data?

What type(s) of access does offshore staff have? no access, standard/non-privileged, privileged/administrative access, other
What access method(s) do offshore contractors use to access state systems? secure VPN (e.g., F5, Cisco AnyConnect), remote desktop / VDI Gateway, privileged access management (PAM) (e.g., Beyond Trust, CyberArk), browser based secure access gateway / zero-trust broker (e.g., ZTNA, Azure Bastion), remote support tools (e.g., TeamViewer, AnyDesk), SSH / RDP via approved management interface, other
Does the agency ensure that current offshore IT services and any future offshore services use phishing resistant MFA when accessing state systems?
What type of data is accessed offshore? metadata, internal, restricted or critical (level 3 or above), regulated (HIPAA, FTI, CJIS, PCA, FERPA, etc.), full database (DB), logs, not applicable, other
What services are performed offshore? administrative support, application / infrastructure hosting, data storage / processing, development (applications, coding, infrastructure, etc.), incident response or data recovery, support services, quality assurance (QA), other