State of Oregon

Cyber Security Services

Cyber Security Responsibilities

2022

ENTERPRISE
information services

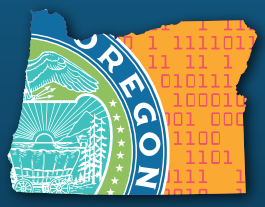
Cyber Security Responsibilities	EIS			
	CSS	CTO	DCS	Agency
Vulnerability Management				
Tenable Vulnerability Scanning				
Determine/Assess deployment requirements	AR		C	CI
Provide hardware/software	AR		C	
Implement scanning	R		I	AR
Enterprise reporting	AR			CI
Vulnerability remediation	CI			AR
Public-Facing Vulnerability Scanning (CISA CyHy)				
Ensure all routable IP address space for the state is being scanned	AR		C	
Ensure all routable IP address space for agency is being scanned	A		C	R
Maintain agency distribution list (DL) for reporting, technical contact, and scan window restrictions	CI			AR
Maintain service with CISA	AR			CI
Vulnerability remediation	CI			AR
Tenable Web Application Scanning				
Determine/Assess deployment requirements	AR			CI
Provide hardware/software (where applicable)	AR		C	CI
Implement scanning	R			AR
Enterprise reporting	AR			
Vulnerability remediation	CI			AR
External Web Application Scanning (CISA WAS)				
Ensure all external web applications for the state are being scanned	AR			CI
Ensure all external web applications for agency are being scanned	A			R
Maintain agency distribution list (DL) for reporting, technical contact, and scan window restrictions	CI			AR
Maintain service with CISA	AR			CI
Vulnerability remediation	CI			AR
Penetration Testing				
Request Pen Testing	CI			AR
Define scope of pen testing activities	CI			AR
Provide resource availability (people, technology, documentation)	CI			AR
Conduct penetration testing activities	AR			CI
Reporting results	ARC			I

Cyber Security Responsibilities	EIS			
	CSS	CTO	DCS	Agency
External Vulnerability Scanning and Validation Testing				
Request scanning	CI			AR
Provide assessment questionnaire and rules of engagement to agency	AR			CI
Respond & Return questionnaire & agree to rules of engagement to agency	CI			AR
Provide Resource Availability (people, technology, documentation)	CI			AR
Perform technical testing per the rules of engagement	AR			CI
Reporting results	AR			I
Cyber Threat Intelligence (CTI) Feeds				
Receive, store, aggregate, and disseminate information specific to cyber threats	AR		I	I
Apply to security operations where applicable	AR		R	R
Monitoring and Detection				
Security Information and Event Management (SIEM)				
Provide enterprise-level collection of security events for detection and after-the-fact incident response	AR			CI
Collect and apply threat intelligence (MS-ISAC, CISA, IBM X-Force, etc.)	AR			
Ensure SOC has contact information for agency notifications	CI			AR
Notify agencies of anomalous activity for action to be taken by agency	AR			CI
Network Security Monitoring and Analysis (MS-ISAC Albert)				
Maintain enterprise service with MS-ISAC (network threat detection at the perimeter)	AR			
Triage reported events and escalate to agencies where applicable	AR			CI
Provide event status and ticket closure requests to MS-ISAC	AR			CI
Phishing Email Analysis				
Report suspected phishing emails to the CSS SOC	CI			AR
Leverage M365 capabilities to assess/investigate reported email	AR			
DNS Filtering: Malicious Domain Blocking and Reporting				
Maintain service with the MS-ISAC	AR		CI	I
Configure agency DNS recursion for service integration	C		CI	AR
Incident Response				
Incident Response Coordination and Management				
Maintain Agency Incident Response (IR) Plan	CI			AR
Maintain Enterprise Incident Response (IR) Plan	AR			CI
Notify CSS SOC of any incident and provide updates	CI			AR
Handle statutory-required notifications to LFO	AR			CI
Assist and/or lead all levels of incident response as needed	AR			CI

Cyber Security Responsibilities	EIS			Agency
	CSS	CTO	DCS	
Cyber Incident Tabletop Exercises (SOC)				
Provide opportunities for agencies to exercise Incident Response Plans and security incident decision-making capabilities	AR			CI
Exercise Agency Incident Response Plan	CI			AR
Enterprise Log Collection and Retention				
Identify security events to be collected (including retention)	CI		AR	I
Manage collection and retention of identified security events	AR		CI	
Awareness and Training				
Annual Security Training				
Provide the Annual Security Training in the LMS	AR			I
Provide access to the LMS and time for staff to take the training	I			AR
Security Awareness				
Provide Security Awareness material (including October Cybersecurity Awareness month)	AR			I
Support, disseminate, and publish the materials	CI			AR
Provide time for staff to participate	I			AR
Phishing Simulation Campaigns				
Onboarding	AR			CI
Deploy requirements	CI			AR
Deploy Phish Alert Button (PAB)	I		C	AR
Prevent spam filtering of simulation emails	I		C	AR
Phishing simulation templates	AR			I
Repeat responder awareness trainings	AR			I
Repeat responder remediation	I			AR
Risk Assessment				
Risk Assessment				
Ensure agencies are scheduled for bi-annual security risk assessments	AR			I
Coordinate and perform bi-annual Security Risk Assessment	AR			CI
Participate in the Security Risk Assessment	CI			AR
Remediate Security Risk Assessment findings	I			AR
Report 3rd party assessments to CSS	I			AR
Security Standards				
Cyber Security Plans (System Security, Agency Vulnerability Management and Incident Response)				
Create and maintain plan template	AR			IC
Develop and maintain plan	CI			AR
Validate plan	R			A

Cyber Security Responsibilities	EIS			Agency
	CSS	CTO	DCS	
Security Standards (e.g. Statewide Standards & CIS Controls)				
IT Procurements/Renewal	RCI			AR
Business Case Security Review	CI			R
Review of 3rd party assessment (e.g. SOC2 Type2)	CI			AR
Audit/Assessment Remediation (e.g. POAMS)	RCI			AR
Network Security				
VPN - SSL and IPSec (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I
Proxy (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I
SSL Termination (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I
Load Balancing (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I

Cyber Security Responsibilities	EIS			Agency
	CSS	CTO	DCS	
Firewall (add, change, remove)				
Deployment requirements	AR			CI
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I
Network Intrusion Detection and Prevention Systems (IDS/IPS) - perimeter				
Provide hardware/software	AR	CI	CI	
Implement	AR		CI	CI
Monitor	AR		I	I
Availability	AR		R	CI
Maintenance	AR		I	I



ENTERPRISE
information services