State of Oregon

Human Risk Management - Information Security Awareness and Training Program Plan

ENTERPRISE
information services

TABLE OF CONTENTS

INTRODUCTION

Enterprise Information Services (EIS) Cyber Security Services (CSS) has developed the Information Security Awareness and Training Program Plan (herein referred to as, "awareness program"). The awareness program is a continuous effort to empower the state's workforce to adopt good security habits at work, at home, and while mobile. The goal of the awareness program is to reduce human vulnerabilities that could result in a breach of confidentiality, integrity, and/or availability of state information assets, thereby increasing the overall security posture of the state.

The awareness program consists of the following implementations and components:

1. **Information Security Awareness Training**
2. **Social Engineering Awareness**
3. **Additional Training and Guidance**

The awareness program is managed under the State Chief Information Officer (CIO) through the Information Awareness Program Coordinator, supported by input from a dedicated advisory board as needed. The advisory board is a cross-agency, cross-functional team, with key members representing a variety of key business roles and operational streams. Agencies, at their own discretion, may also implement an awareness program coordinator specific to their agency to assist in agency-wide awareness program integration and compliance.

Effective human risk mitigation and management is an essential component to ensure the security of the state's information systems and information assets. Even with the most current and advanced technological security integrations, agencies are still at risk from cyber threats resulting from human error. Reducing the risk of such human errors is critical to ensuring that the state can continue to serve Oregonians effectively and remains a critical component to ensuring the security of state information assets. Effectively mitigating human risk is the sole purpose of the awareness program.

AUTHORITY

ORS 276A.300(2):

"The State Chief Information Officer has responsibility for and authority over information systems security in the executive department, including responsibility for taking all measures that are reasonably necessary to protect the availability, integrity, or confidentiality of information systems or the information stored in information systems. The State Chief Information Officer shall, after consultation and collaborative development with agencies, establish a state information systems security plan and associated standards, policies, and procedures. The plan must align with and support the Enterprise Information Resources Management Strategy described in ORS 276A.203 (State Chief Information Officer)."

ORS 276A.323(2):

"All state agencies shall: (a) cooperate with the office of Enterprise Information Services in the implementation of a continuing statewide agency-by-agency risk-based information technology security assessment and remediation program, (b) cooperate in the development of, and follow, the plans, rules, policies and standards opted by the State Chief Information Officer with regard to the unification of agency information technology security functions in this state, (c) conduct and document the completion of annual information security awareness training for all employees, (d) report security metrics using methodologies developed by the office of Enterprise Information Services, and (e) participate in activities coordinated by the office of Enterprise Information Services in order to better understand and address security incidents and critical cybersecurity threats to the state."

Statewide IT Policies, Procedures, and Guidance:

The State Chief Information Officer, through EIS, establishes and maintains statewide information technology policies, procedures, standards, and guidance. These cover information systems security, risk management, and related areas under authority of ORS 276A.300 and 276A.323. All agencies must comply with these directives, which are updated periodically to reflect changing requirements. The current and authoritative versions are maintained centrally by EIS. See the official EIS policies and resources page for the latest versions:

https://www.oregon.gov/eis/Pages/policies.aspx

APPLICATION

The awareness program applies to all Executive Branch agencies as defined in ORS 174.112, except as provided in ORS 276A.300 and OAR125-800 and as they apply to the State Board of Higher Education and the Oregon University System, the Oregon State Lottery, Secretary of State, State Treasurer, and the Attorney General.

TERMS AND DEFINITIONS

Agency. Any executive branch board, commission, department, division, office, or other organizational entity within the state government that operates under the authority of the state of Oregon.

Asset. Anything that has value to an agency, including digital, physical, or intellectual property.

Availability. Ensuring timely and reliable access to and use of information (see "Information").

Awareness Program. The Human Risk Management Program: A structured effort aimed at increasing employee knowledge and awareness of cybersecurity best practices to effectively mitigate human risks (see "Cybersecurity" and "Human Risk").

Compliance Metrics. Measurements used to assess statewide adherence and compliance to the requirements outlined in the awareness program plan and evaluate the overall effectiveness of the awareness program.

Confidentiality. Preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information (see "Information").

Cybersecurity. The process of protecting information systems and information assets (see "Information System" and "Information Asset").

Human Risk. Risk associated with human error or behavior that could lead to a security incident (see "Risk" and "Security Incident").

Information. Any communication or representation of knowledge in any medium or form. Examples include, but are not limited to:

- Documents, reports, statistics, files, and records compiled or stored in digital or physical form
- E-mails or messaging system conversations and their attachments
- Audio and video files
- Images, graphics, pictures, and photographs
- Programs, software, and macros

Information Asset. Any information that has value to the agency.

Information Security. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (see "Information System" and "Integrity").

Information Security Awareness Training. The mandatory, year-round security education program required by ORS 276A.323 and DAS Policy 107-004-052 for all individuals with access to Oregon Executive Branch information assets. It is satisfied by completing required training modules (delivered annually, quarterly, or in another recurring cadence as designated by Cyber Security Services).

Information Security Event. An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.

Information System. Computer, hardware, software, storage media, networks, operational procedures, and processes used in collecting, processing, storing, sharing, or distributing

information within, or with any access beyond ordinary public access, to the state's shared computing and network infrastructure.

Integrity. Guarding against improper information modification or destruction, which ensures information non-repudiation and authenticity.

Learning Management System (LMS). Software application for the administration, documentation, tracking, reporting, and delivery of educational courses or training programs.

Phishing. A fraudulent attempt, typically via email or message, intended to deceive individuals into disclosing sensitive information or performing an action they would not otherwise perform that may compromise security.

Security Incident. Unwanted or unexpected information security event(s) that result in harm or pose a significant threat of harm to information assets and require non-routine preventative or corrective action events.

Smishing. A category of phishing attack that involves the use of Short Message Service (SMS) text messaging as a medium for the social engineering attack (see "Social Engineering Attack").

Social Engineering. The art of exploiting human psychology to manipulate individuals to reveal confidential information or perform actions that they would not otherwise perform that may compromise security.

Social Engineering Attack. An effort to compromise the state's cybersecurity posture and breach the confidentiality, availability, or integrity of state information assets or systems using social engineering, including phishing and smishing.

Social Engineering Awareness Program. Structured exercises and simulations designed to educate and evaluate workforce susceptibility to social engineering attacks.

Phishing Awareness Program. Structured exercises and simulations designed to educate and evaluate workforce susceptibility to phishing attacks.

Privileged Access. Access to any information system that enables the user to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access implies greater access than the average end-user (see "User").

Privileged User. A user who has been granted privileged access (see "User").

Risk. A measure of the extent to which an organization is threatened by a potential circumstance or event, which considers the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

User. Any individual authorized to access or interact with state information assets, systems, or networks, including employees, contractors, volunteers, board or commission members, and any third-party personnel.

ROLES

Agency Awareness Program Coordinator. Responsible for agency-wide integration and compliance with the awareness program. This role only exists in agencies that choose to implement such a role based on their own discretion and budgetary limitations.

Advisory Board. Cross-agency group tasked with oversight and strategic planning of the awareness program, providing feedback on awareness program effectiveness as needed or requested by the Information Awareness Program Coordinator (see "Information Awareness Program Coordinator").

Agency Director. Executive responsible for actively analyzing, managing, and enforcing their agency's compliance with statewide standards, policies, procedures, regulations, and guidelines, including human risk management provisions, as required.

Agency Management. Responsible for complying with all the requirements for agency management set forth in statewide standards, policies, procedures, regulations, and guidelines, including enforcing human risk management provisions amongst the employees they manage, as required.

Cyber Security Services (CSS). The entity within Enterprise Information Services (see "Enterprise Information Services") responsible for statewide cybersecurity oversight, including developing, managing, and implementing cybersecurity policies, security incident response coordination, security assessments, and security awareness programs.

Enterprise Information Services (EIS). Agency responsible for statewide information technology management, policy oversight, and the implementation of statewide cybersecurity awareness programs.

Information Awareness Program Coordinator. Responsible for the overall coordination and management of the information awareness program at the enterprise level.

State Chief Information Officer (CIO). Leads state government in enterprise information technology management, strategic planning, and policy.

State Chief Information Security Officer (CISO). Responsible for statewide information security.

Privileged User. A user who has been granted privileged access to a state information system or information asset is responsible for complying with all the requirements for privileged users set forth in statewide standards, policies, procedures, plans, regulations, and guidelines. This includes compliance with the required information security awareness training and the proper reporting of real and simulated social engineering attacks (i.e. phishing emails) according to statewide standards, policies, procedures, and plans, and adherence to any additional training requirements for privileged users.

User. Responsible for complying with all the requirements set forth for users in statewide standards, policies, procedures, plans, regulations, and guidelines. This includes compliance with the required information security awareness training and the proper reporting of real and simulated social engineering attacks (i.e. phishing emails) according to statewide standards, policies, procedures, and plans.

PROGRAM

The awareness program's objective is to reduce human risk across the enterprise. To achieve this objective, the awareness program consists of three primary implementations and components:

1. **Information Security Awareness Training**
2. **Social Engineering Awareness Program**
3. **Additional Training and Guidance**

Information Security Awareness Training

ORS 276A.323 requires annual information security awareness training for all employees, board and commission members, temporary employees, contractors, volunteers, and all third-party personnel who have access to state information systems or information assets ("users"). This statutory requirement is limited to Executive Branch agencies as defined in ***ORS 174.112*** but is not limited to those with state system access. It includes all individuals with access to state information assets, including all written, verbal, and electronic information.

The goal of the required information security awareness training is to provide foundational information security training for all users and to comply with all state and federal policies, standards, and statutes that govern requirements and guidelines for the delivery and completion cadence of information security awareness training for the Executive Branch.

Information security awareness training must be completed by users by December 31st each calendar year. This training is made available and assigned to all users by CSS as soon as feasible during the beginning of each calendar year, but no later than March 31st. For users gaining access for the first time, they are required to complete the required information security awareness training within 30 calendar days of receiving access to state information systems or state information assets. Such users gaining access for the first time are only required to complete the training once in the calendar year that they receive access unless otherwise directed by CSS. Agencies are responsible for incorporating the completion of the required information security awareness training into their onboarding and continual training process. Managers are responsible for ensuring and verifying their employees have completed the training by the required due date.

A user who is unable to complete the required information security awareness training using the LMS for any reason other than a technological or technical issue should follow *the Information Security Training – Alternative Formats* instructions, accessible from the CSS website. Those experiencing a technological or technical issue that prevents them from completing information security awareness training should reach out to their immediate supervisor, their agency awareness program coordinator, their agency Information Technology (IT) help desk, or email security.training@das.oregon.gov for further instructions before completing the alternative format as a substitute.

Social Engineering Awareness

Social engineering remains the number one attack vector for cybercriminals because it often leads to success. State of Oregon employees are often a target because they have access to sensitive and confidential information and access to state information systems and assets. As a result,

mitigating enterprise susceptibility to social engineering attacks is a critical objective that the Social Engineering Awareness Program has been developed to achieve. The Social Engineering Awareness Program is an adaptive training program that allows for simulated social engineering attacks to be sent to users repeatedly throughout the year, increasing enterprise awareness and knowledge of social engineering attacks and encouraging proper responses to such attacks.

The Social Engineering Awareness Program helps identify which users are susceptible to social engineering attacks and provides the opportunity for more focused training opportunities for those users to better mitigate organizational risk.

Emerging social engineering threats and attacks may result in changes and updates to the Social Engineering Awareness Program, including the addition of other awareness integrations such as smishing, in accordance with the guidelines provisioned in the "Program History, Governance, and Sustainability" section of this awareness program plan. The Phishing Awareness Program is the primary component of the Social Engineering Awareness Program.

Phishing Awareness

All users will receive a simulated phishing email each month of varying difficulty. Difficulty levels represent increasing sophistication, complexity, and realism in simulated phishing emails. Higher-level simulations (4-5) mimic advanced cyber-attacks. The simulation levels a user receives will be considered when targeted reinforcement training is recommended or assigned to users based on their susceptibility to phishing attacks.

Simulated phishing emails are categorized based on difficulty according to the following scale:

1. Level 1 (Easy)
2. Level 2 (Basic)
3. Level 3 (Moderate)
4. Level 4 (Advanced)
5. Level 5 (Hard)

Users must follow the reporting process in accordance with statewide standards, policies, procedures, and guidelines if they believe they have received a real or simulated phishing email.

Additional Training and Guidance

Required Information Security Awareness Training Social Engineering Awareness are not enough to optimally reduce human risk across the enterprise. As a result, the awareness program will continuously reinforce key behaviors by utilizing various other methods throughout the year. Additional training and guidance materials will be delivered, at a minimum, once per quarter, and ad-hoc throughout the year to address emerging threats or compliance gaps and consist of the following materials:

- **Security Awareness Videos**: Dissemination of awareness videos to users. These videos will be distributed by email to agency management and leadership and made available to all users.
- **Digital Signage**: Dissemination of information security awareness media to users. These media will be distributed by email to agency management and leadership and made available to all users. This media could consist of a variety of formats including:

    - Digital Posters
    - Printable Posters and Informative Signage
    - Information about Relevant Cybersecurity Seminars and Info Sessions
- **Targeted Training for Privileged Users**: Privileged users pose greater human risk to the enterprise because of their escalated privilege and their access to, potentially, more confidential information assets. Various mandatory and optional training activities and media may be distributed to agency management and leadership throughout the year that will then be provided to privileged users.
- **CSS-hosted Information Security Informative Training Events**: Throughout the year, CSS may host ad-hoc information security informative training events remotely in which users may choose to attend or may be required to attend by agency management or CSS.
- **EIS Periodical Material**: While not distributed directly by CSS, EIS frequently posts periodical security and information technology material on the EIS website throughout the year in a variety of forms that often contains valuable information involving cyber security best practices and security awareness materials that users can review on their own accord.

METRICS

It is important to test and measure if the awareness program is an effective method of educating users and changing behaviors. The awareness program will focus on various metric categories that measure the effectiveness of the awareness program throughout the year. Metrics will be used to analyze the overall security posture of the state and may be analyzed to make various changes to more effectively implement and improve the awareness program and to ensure the program is meeting its goals.

CSS will organize and analyze collected enterprise-level metrics quarterly or annually, depending on the metric, and communicate findings to agency leadership. Agencies are responsible for reviewing the findings and taking appropriate actions based on identified trends.

These metrics may change based on emerging industry standards, federal guidance, statutory regulations, and various other factors. Enterprise-level metrics will be made available to agency leadership and agency directors quarterly or annually, depending on the metric, so agency leadership and agency directors can assess their agency's security posture and compare it to the enterprise.

At a minimum, CSS will collect, analyze, and distribute the following enterprise-level metrics annually:

1. **Information Security Awareness Training Completion** (number and percentage of users who complete the annual information security awareness training by the required due date)

In addition to the minimum enterprise-level metrics listed above that will be distributed annually, various other enterprise-level compliance metrics will also be distributed to agencies quarterly, including compliance metrics pertaining to the Social Engineering Awareness Program. Quarterly metrics that are collected, analyzed, and distributed to agencies are subject to change at the discretion of the Information Awareness Program Coordinator, in collaboration with the dedicated

advisory board. Examples of enterprise-level metrics that may be collected, analyzed, and disseminated quarterly include:

1. **Phishing Susceptibility Rate** (% of users clicking links or otherwise improperly engaging with a simulated phishing email)
2. **Reporting Accuracy Rate** (% of users who correctly report simulated phishing emails according to statewide policy, procedure, standards, and guidelines)
3. **Repeat Failure Rate** (% of users who fail multiple simulations in a single calendar year)
4. **Enterprise Engagement and Interaction Rate with Additional Training and Guidance Materials** (% of users who attend or engage with additional training and guidance sessions or materials)

PROGRAM PLAN HISTORY, GOVERNANCE, AND SUSTAINABILITY

Program Plan History

Version History	Effective Date	Authors
HRM-ISAT Program Plan 1.0	05/2022	CSS
HRM-ISAT Program Plan 2.0	12/2026	Timothy Marshall, Jake Wilson

Program Plan Governance

This plan will be updated as needed to accurately reflect the current goals, objectives, and components of the awareness program. The CSS team will, at minimum, biennially review this plan for updates and changes and make such updates and changes as needed. This program plan may also be updated ad-hoc to more accurately or clearly align the plan with the current goals, objectives, and components of the awareness program.

Program Plan Sustainability

Ensuring that the awareness program effectively meets its goal of reducing enterprise human risk is a constant effort. To ensure the awareness program stays effective, relevant, and sustainable, various factors may influence the updating of the awareness program, including but not limited to:

1. Compliance Metrics Analysis
2. Emerging Cybersecurity Threats
3. Federal or State Statutes, Regulations, Policies, or Standards
4. Feedback from Agencies
5. Direction From the State CIO or CISO

This program plan will be updated as needed when the awareness program is updated.

APPENDIX A – PROCEDURES

INFORMATION SECURITY AWARENESS TRAINING PROCEDURE

RESPONSIBILITY	STEP	ACTION
Cyber Security Services (CSS)	1	Create, publish, and distribute the required information security awareness training by March 31st.
All Users	2	Complete the required information security awareness training by December 31st or, if a new user, within 30 days of receiving access to state information asset(s) or system(s).
Privileged Users	3	Complying with any additional required information security training for privileged users as provisioned by CSS.
Agency Management	4	Ensure the employees that they manage have completed the required information security awareness training by the due date.
CSS	5	Collect, analyze, and distribute the required information security awareness training metrics annually, at a minimum.
Agency Director	6	Analyze and take corrective actions based on identified trends found in the required information security awareness training metrics.
Agency Awareness Program Coordinator (if applicable)	7	Analyze the agency's compliance with Steps 2, 3, 4, and 6. Take corrective action as necessary to ensure the agency's compliance with Steps 2, 3, 4 and 6.
Information Awareness Program Coordinator (CSS)	8	Analyze statewide compliance with Steps 1-6. Take corrective actions as necessary to ensure statewide compliance with Steps 1-6.
Advisory Board	9	Collaborate with the Information Awareness Program Coordinator for the oversight and strategic planning of the required information security awareness training as requested by the Information Awareness Program Coordinator.

SOCIAL ENGINEERING AWARENESS PROCEDURE

RESPONSIBILITY	STEP	ACTION
Cyber Security Services (CSS)	1	Send phishing simulation emails at random monthly intervals to users' state email addresses.
All Users	2	Report simulated and real phishing emails according to statewide standards, policies, plans, and procedures.
Agency Management	3	Ensure the employees that they manage are aware of how to identify phishing emails and how to report phishing emails according to statewide standards, policies, plans, and procedures.
CSS	4	Collect, analyze, and distribute phishing awareness program metrics quarterly or annually, depending on the metric, at a minimum.
Agency Director	5	Analyze and take corrective actions based on identified trends found in the phishing awareness program metrics.
Agency Awareness Program Coordinator (if applicable)	6	Analyze the agency's compliance with Steps 2, 3, and 5. Take corrective actions as necessary to ensure agency's compliance with Steps 2, 3, and 5.
Information Awareness Program Coordinator (CSS)	7	Analyze statewide compliance with Steps 1-5. Take corrective actions as necessary to ensure statewide compliance with Steps 1-5.
Advisory Board	8	Collaborate with the Information Awareness Program Coordinator for the oversight and strategic planning of the social engineering awareness program as requested by the Information Awareness Program Coordinator.

RESPONSIBILITY	STEP	ACTION
Cyber Security Services (CSS)	1	Create, publish, and distribute additional training and guidance material, quarterly, at a minimum.
All Users	2	Review additional training and guidance material as needed to refresh best security practices and behaviors.
Agency Management	3	Ensure the employees that they manage are aware of where to find and how to access additional training and guidance material and ensure that employees review material according to any provisions or requirements outlined in statewide standards, policies, or procedures.
CSS	4	Collect, analyze, and distribute additional training and guidance material metrics.
Agency Director	5	Analyze and take corrective actions based on identified trends found in the additional training and guidance metrics.
Agency Awareness Program Coordinator (if applicable)	6	Analyze the agency's compliance with Steps 2, 3, and 5. Take corrective actions as necessary to ensure agency's compliance with Steps 2, 3, and 5.
Information Awareness Program Coordinator (CSS)	7	Analyze statewide compliance with Steps 1-5. Take corrective actions as necessary to ensure statewide compliance with Steps 1-5.
Advisory Board	8	Collaborate with the Information Awareness Program Coordinator for the oversight and strategic planning of additional training and guidance as requested by the Information Awareness Program Coordinator.