

Procedures/Standards Update

PS016_2021

November 2021

TO:

Chief Information Officers (CIO)
Information Security Officers (ISO)
Agency Chief Information Officers (AIO)
Agency Information Security Officers (AISO)

SUBJECT: PHISHING EXERCISE STANDARD

BACKGROUND

The California Department of Technology (CDT) Office of Information Security (OIS) released the Phishing Exercise Standard in October 2020. The Statewide Information Management Manual (SIMM) 5320-A includes the requirements to assist agencies/state entities coordinate and execute simulated phishing exercises in compliance with State Administrative Manual (SAM) Section 5320. The policy provides specific direction and additional guidance on conducting phishing exercises at regular intervals to ensure agencies/state entities can obtain a direct measurement of an employee's understanding, as well as progress in user behavior to reduce the number of security incidents and malware attacks to state IT infrastructure.

Agencies/state entities must ensure that phishing exercises are conducted and comply with the requirements outlined in SIMM Section 5320-A.

PURPOSE

The purpose of this Procedures/Standards update is to announce:

- Updated SIMM Section 5320-A, to include additional phishing techniques and exercise planning coordination requirements for agencies/state entities when coordinating and executing phishing exercises with CDT's OIS and the California Cybersecurity Integration Center (Cal-CSIC).
- Effective immediately, agencies/state entities must implement the updates. Any exceptions or variations below these standards must be documented and supported by the state entity variance policy and risk assessment process outlined in SAM 5305.7, and a Plan of Action and Milestones (POAM) when applicable.

REFERENCES

The following reference materials are associated with this Procedures/Standards Update.

SIMM is available on CDT's website located at <https://cdt.ca.gov/policy/simm/>.

SAM is available on the Department of General Services' website located at

<https://www.dgs.ca.gov/Resources/SAM/TOC>.

- SAM Section 5320
- SIMM Section 5320-A

QUESTIONS:

Direct questions regarding this announcement to the Department of Technology, Office of Information Security at security@state.ca.gov.