GENERAL OFFICE MEMORANDUM 22-014

TO: ALL DISTRICT ATTORNEY PERSONNEL

FROM: SHARON L. WOO SW
Chief Deputy District Attorney

SUBJECT: MANDATED SECURITY AWARENESS TRAINING

DATE: FEBRUARY 7, 2022

Board of Supervisors Information Technology Policy 6.100 requires that the County Chief Information Security Officer (CISO) establish and maintain a Countywide Information Security Awareness training program based on the County's information security policies. It further requires that Countywide Information Security Awareness training be conducted annually throughout a Workforce Member's term of employment.

To meet this requirement, the CISO issued Technology Brief 22-01 (2022 Cybersecurity Awareness Training), requiring all County employees take nine (9) security awareness courses using a training service called Infosec IQ. The courses have a total completion time of 43 minutes and are identified below:

• Core Concepts: Incident Response	5:27 mins
• Core Concepts: MFA	3:53 mins
• Just the Facts: Safe Web Browsing	5:08 mins
• Just the Facts: Insider Threats	4:55 mins
• Just the Facts: Public Wi-Fi	5:10 mins
• Just the Facts: Ransomware	3:43 mins
• Just the Facts: Working Remotely	3:48 mins
• Need to Know: Physical Security	4:15 mins
• Need to Know: Social Engineering	4:05 mins

Courses can be taken separately and in any order as long as they are completed by June 30, 2022. Additionally, Infosec IQ will be used to conduct phishing exercises and training throughout the year.

The information available within these courses will minimize potential cybersecurity risks associated with teleworking and help secure the Department's applications and networks. All employees should begin taking these courses now to complete by the required time.

LADA employees will receive an email from Infosec IQ Notifications (notifications@securityiq-notifications.com) informing them that they are enrolled in the courses. Click the "Start your training" button to initiate the training. Each course will start automatically once the previous course ends.

Technology Brief 22-01 is attached for your reference. Questions regarding the training requirements or the courses should be directed to Nhan Le, Departmental Information Security Officer, at nle@da.lacounty.gov or (213) 344-2454.

nl

Attachment

Office of the CIO

Technology Brief

NUMBER:

TB 22-01

SUBJECT:

2022 Cybersecurity Awareness Training

DATE PUBLISHED: January 18, 2022	DATE REVISED:
EXPIRES: JUNE 30, 2022	
CIO PROGRAM: INFORMATION SECURITY	

REFERENCES: Board Policy 6.100 – Information Security Policy, Information Security Awareness Training

Distribution

Chief Deputies, Admin Deputies, Technology Management Council (TMC), Information Security Committee (ISC), and Departmental Training Coordinators

Purpose

Provide Cybersecurity Awareness Training related to the current threat landscape and increase workforce member awareness to minimize County risk and information security exposure.

Executive Summary and Context

Board Policy 6.100 requires all workforce members to complete information security awareness annually.

The Chief Information Security Officer has selected nine (9) core modules that all workforce members must complete based on industry frameworks, cybersecurity and privacy best practices, county policy, and relevant county threats.

Phishing email simulations are a part of cybersecurity awareness. The intent behind phishing email simulations is to exercise and practice proper identification of suspicious emails and report those emails following established procedures.

Strategic Assumptions

This Technology Brief supports Board Policy 6.100 – Information Security Policy, Information Security Awareness Training

Key Considerations

Information Security Awareness Training is vital for protecting the County's information assets, minimizing the risk of workforce members being victims of cyber-attack, and subsequently a breach of confidential information.

Approach

On January 18, 2022, all workforce members will be required to complete all assigned mandatory Information Security Awareness Training by June 30, 2022. All mandatory training will be deployed automatically by the Department of Human Resources using the County's Learning Link platform.

Nine (9) mandatory information security awareness modules have been selected and will take approximately forty-three (43) minutes to complete. This list of the training modules are as follows:

1. Core Concepts: Incident Response
2. Core Concepts: MFA
3. Just the Facts: Safe Web Browsing
4. Just the Facts: Insider Threats
5. Just the Facts: Public Wi-Fi
6. Just the Facts: Ransomware
7. Just the Facts: Working Remotely
8. Need to Know: Physical Security
9. Need to Know: Social Engineering

All new 2022 Workforce Members shall be assigned and complete the nine mandatory training within one month of employment.

Email phishing simulations are to be used as additional awareness training for the Workforce Members. Departments are required to deploy at least four (4) department simulated phishing campaigns. ISD Cyber Governance and Operations Branch is required to deploy at least four (4) countywide simulated phishing campaigns. Both department (4) and countywide (4) phishing email campaigns must be completed by December 30, 2022.

Approved

Jan 12, 2022

Peter Loo, Acting Chief Information Officer
County of Los Angeles

Date

Jan 12, 2022

Jeff Aguilar, Acting Chief Information Security Officer
County of Los Angeles

Date