GENERAL OFFICE MEMORANDUM 19-088

TO: ALL DISTRICT ATTORNEY PERSONNEL

FROM: JOSEPH P. ESPOSITO
Chief Deputy District Attorney

SUBJECT: MANDATED SECURITY AWARENESS TRAINING

DATE: AUGUST 15, 2019

The 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 has issued a Technology Directive requiring all County employees take nine (9) security awareness courses using a training service called KnowBe4. Courses can be taken separately, in any order, as long as all courses are completed by October 15, 2019. Additionally, the KnowBe4 service will be utilized to conduct phishing exercises and training throughout the year.

The nine courses are identified below and have a total completion time of 92 minutes.

1. Security Awareness Fundamentals
2. Creating Strong Passwords
3. Social Engineering Basics
4. Understanding and Protecting PII
5. Encryption
6. Data Disposal
7. Privacy Basics
8. Using the Phish Alert Button
9. Mobile Security Basics

The information available in these courses has already proven valuable in avoiding potential cybersecurity incidents within this department. Employees should begin taking courses early to ensure courses are completed by the deadline.

Employees will receive an email from KnowBe4 (do-not-reply@knowbe4.com) informing them that they have been enrolled in training. Within the email is a link that will direct users to confirm their account using their LADA email address. All LADA user accounts within KnowBe4 were previously created by the Bureau of Administrative Services, Systems Division.

After confirming their account, users may start the training. For more information with regards to this process, a step by step guide can be found at https://support.knowbe4.com/hc/en-us/articles/204469068-Enrolled-in-Training-A-4-Step-Guide-to-Getting-Started.

Technology Directive 19-01 is attached for reference. Questions regarding this training requirement or the courses should be directed to the Office's Departmental Information Security Officer, Nhan Le, at nle@da.lacounty.gov or (562) 403-6668.

nl

Attachment

Office of the CIO

Technology Directive

NUMBER:	
TD 19-01	

SUBJECT:	DATE ISSUED:	DATE REVISED:
Cybersecurity Awareness Training	January 24, 2019	
	EXPIRES: UNLESS RESCINDED SUPERSEDES TD 17-02	
	CIO PROGRAM: INFORMATION SECURITY	

REFERENCES:

Board Policy 6.100 – Information Security Policy

ISO/IEC 27002 Information Technology – Security Techniques – Code of Practice for Information Security Controls

Center for Internet Security – 20 Critical Controls

National Institute of Standards and Technology (NIST) – Framework for Improving Critical Infrastructure Cybersecurity (CSF) v. 1.1

Distribution

Chief Deputies, Admin Deputies, Technology Management Council (TMC), Information Security Committee (ISC)

Purpose

Ensure compliance with County Board of Supervisors Policy 6.100 and minimize the risk of employee error resulting in an information security exposure thus improving the protection of County Information Assets.

This Technology Directive supersedes TD 17-02 issued November 9, 2017 and expired December 31, 2018.

Background & Context

Board Policy 6.100 adopted in November 11, 2018 states:

> ***"Information Security Awareness Training***
>
> *The Chief Information Security Officer, in cooperation with the DISOs, will establish and maintain a countywide Information Security awareness training program based on the County's information security policies.*
>
> *County Departments may develop additional Information Security awareness training programs based on their specific needs, legal requirements and sensitivity of information.*
>
> *Countywide Information Security awareness training shall begin with Workforce Member new hire orientation and shall be conducted annually throughout a Workforce Members term of employment.*

Information Security awareness training shall be provided to Workforce Members as appropriate to their job function, duties, and responsibilities.

Each County Department shall ensure that its Workforce Members participate in the countywide Information Security awareness training program. Workforce Member participation in Information Security awareness training should be documented."

To support Board Policy 6.100, in 2018 the Office of the Chief Information Security Officer (OCISO) purchased cybersecurity awareness training content from KnowBe4 to replace previously used online cybersecurity training content. The previously available training did not provide sufficient awareness content related to threats to County information assets and proper mitigation strategies.

Appropriate modules have been selected to ensure that all workforce members obtain sufficient information to increase their awareness of common cybersecurity threats and how to address such threats.

There are currently over 600 course modules available in the KnowBe4 Learning Management System (LMS). The OCISO has selected nine (9) core modules that all workforce members must complete based on industry frameworks and best practices, county policy and relevant experience and research. Departmental Information Security Officers (DISOs) may coordinate with the OCISO and departmental training coordinators to make additional cybersecurity courses available for their department employee's training program. All courses are currently available for review by authorized departmental personnel within the KnowBe4 LMS.

KnowBe4 also includes a "Report Phishing" button (known as the Phish Alert Button or PAB) that will appear in all Outlook clients (Windows, iOS and Android). Using this button workforce members can immediately report suspected phishing emails to technical support for investigation. ISD will deploy the Phish Alert Button to Tenant A on February 8th.

Acquired content also includes an email phishing simulator. The OCISO plans to conduct two email phishing simulations annually. DISOs are authorized, in coordination with their departmental management, to conduct email phishing simulations as frequently as desired by the department.

Directive

1. County workforce members are required to complete the nine (9) core modules of formal cybersecurity awareness training (courses range in length from 1 to 23 minutes) annually. For example, if a department deploys training to all workforce members starting May 1, 2019, then departmental workforce members must complete training within 12 months. May 1, 2020 would be the start of the following year's cybersecurity awareness training cycle.

2. The nine (9) core modules consists of a total of 98 minutes (1 hour 36 minutes) and are listed below. All modules are required annually as a core set of training for all County workforce members:

    1. Security Awareness Fundamentals
    2. Creating Strong Passwords
    3. Social Engineering Basics
    4. Understanding and Protecting PII
    5. Encryption
    6. Data Disposal
    7. Privacy Basics
    8. Using the Phish Alert Button
    9. Mobile Security Basics

    Workforce members will also be provided a link to a PDF file of all approved information security policies to review.

3. DISOs and Department Training Coordinators may elect to add additional role specific training modules.
4. Countywide email phishing simulation tests will be conducted twice annually by the OCISO.
5. DISOs may conduct additional departmental email phishing simulations to meet department objectives
6. ISD/ITS will deploy the Phish Alert Button (PAB) to all Tenant A clients via O365 on February 8th. This will include Outlook 2016 for Windows (earlier versions of Outlook must be deployed by .msi), Outlook Web Access, and the Outlook Mobile App (Andorid). Plans to deploy PAB to iOS devices is schedule for a later date. DISOs within Tenant A must ensure that the Phish Alert Button is deployed throughout their Department. DISOs outside of Tenant A must coordinate with the OCISO to deploy the Phish Alert Button.

Scope & Applicability	This Technology Directive applies to all County IT Workforce Members and Departments.
Exceptions	Requests for exceptions to this Technology Directive will be reviewed and approved by the County's Chief Information Security Officer or designee. Each exception request must state the justification for the request, potential impacts and risks of granting the exception.
Approved	William S. Kehoe, Chief Information Officer County of Los Angeles Date: 1/24/19