Policy Type: Administrative

Category: Information Technology

Policy Name: Information Privacy and Cyber Security Trainings

Policy Owner: County Executive

Policy Purpose

The purpose of this policy is to ensure all County employees complete, at a minimum, introductory level training courses in information privacy and cyber security to increase awareness of best practices in protecting County information systems and the information the County collects, stores, and processes.

Policy Summary

The County collects, stores, and processes personal and sensitive information to serve the community. The protection of this information is entrusted to the County, and the security of the County's information technology systems is of paramount importance. It is the responsibility of all County employees to safeguard clients' personal and sensitive information.

Each department shall ensure its employees complete, at a minimum, introductory level training courses in information privacy and cyber security, and complete refresher trainings for both courses every calendar year thereafter, unless the department is otherwise exempted in this policy. New employees shall complete information privacy and cyber security training courses within 90 days of their hire and every calendar year thereafter, unless otherwise exempted in this policy. Completion of the trainings required by this policy do not exempt employees from having to complete any additional department-specific training required by their respective departments or other authority.

Department Exemption Requests from Training Requirements
Departments that deploy their own information privacy training and/or cyber security training courses may request an exemption from these training requirements by submitting a request in writing to the following County personnel:

- Chief Privacy Officer, or designee (for information privacy training exemptions)

- Chief Information Security Officer, or designee (for cyber security training exemptions)

Department requests for an exemption will be evaluated by the above personnel in consultation with the Chief Operating Officer and the Office of the County Counsel, and a determination will be made based on the content of a department's training materials and its training requirements (e.g., training frequency). Departments may receive an exemption for relevant staff from one or both training requirements identified by this policy.

If an exemption is approved for a department information privacy and/or cyber security training course, the content and frequency of a department's training must be maintained for the exemption to remain valid. Minor updates to department information privacy and/or cyber security training may be made in consultation with the Chief Privacy Officer and/or Chief Information Security Officer, or their designees. However, a request for an exemption from these training requirements must be re-submitted to the above County personnel when major revisions are made to department training content or requirements.

If a department is unsure whether revisions are considered major or minor, it shall provide details and the purpose of the revisions to the Chief Privacy

Officer (for information privacy training) and/or Chief Information Security Officer (for cyber security training), or their designees, who shall make a final determination on the type of revision (i.e., major or minor) and whether or not a new review of updated department-specific training content and requirements is necessary.

HIPAA Privacy and Security Training Exemption for Employees

Employees who receive annual privacy and security training required by the Health Insurance Portability and Accountability Act ("HIPAA privacy and security training") are exempt from this policy, unless required by their department to also complete the introductory-level privacy training and cyber security training. For purposes of this policy, the HIPAA privacy and security training material and training requirements have been deemed to provide equivalent content and training frequency. Departments whose employees complete annual HIPAA privacy and security training do not need to make a request for an exemption through the process set forth in this policy, and do not need to complete the training described in this policy.

Volunteers and Individual Contractors

Departments may, at their discretion, require volunteers and individual contractors who perform services for their department to complete the privacy training and/or cybersecurity training when volunteers and individual contractors have access to County data systems.

Procedures

Ensuring Compliance with Training Requirements

1) The **Privacy Office and the Information Security Office** shall:

1a) Develop the required training courses from their respective offices, in consultation with the Offices of the County Executive and County Counsel.

1b) Make the required training available on the County's online training platform. For employees who are unable to access the online version of the privacy training course, the Privacy Office will make the course content available in an alternative format, which departments may distribute to their employees and report completion results to the administrators of the County's online training platform.

1c) Review training completion results at least quarterly to determine employees' compliance with this policy's training requirements, and notify a Department Head, or designee, when department employees are out of compliance with the policy. The Privacy Office and/or the Information Security Office may refer any outstanding department compliance issues to the Chief Operating Officer and/or recommend an appropriate measure to reach completion or a course of corrective action.

1d) Provide notice to departments of the deadlines for departments to submit requests for exemptions in subsequent years.

2) The **Department Head, or designee,** shall ensure the department's employees have completed training in accordance with this policy or that their department has received a written exemption from the Chief Privacy Officer and/or Chief Information Security Officer.

Requesting Department Exemption from Training Requirements

1) To request an exemption for either or both trainings, a **Department Head, or designee**, shall submit a written request that includes the content and frequency of the training provided to the department's employees to the Privacy Office (email: PrivacyOffice@ceo.sccgov.org) and/or the Information Security Office (email: o365-iso-team@sccconnect.onmicrosoft.com).

2) The **Chief Privacy Officer and/or Chief Information Security Officer, or their designees**, in consultation with the Chief Operating Officer and Office

of the County Counsel, shall review exemption requests and shall provide a written response within 30 days of the request, unless the time to respond is extended, with either an Approval, Approval with Condition(s), or Rejection, as follows:

- *Approval*: Should an Approval be granted for adequate department-specific training, then the department's employees will not be required to take the training(s) required by this policy.

- *Approval with Condition(s):* An Approval with Condition(s) means that the Privacy Office and/or the Information Security Office mostly agree with the training content and/or requirements submitted in the department's request, but require additional steps to be completed before providing full approval. Departments should address those conditions, consulting with the Privacy Office (for privacy training) or Information Security Office (for security training) as needed, within 30 days of the Approval with Condition(s) written response, or with any extensions agreed to by the department and respective offices. Should these respective offices agree that the appropriate conditions have been met, then the department's employees will not be required to take the trainings required by this policy. If the conditions have not been met within 30 days, or within an agreed upon extension period, then that department's employees must take the trainings required by this policy.

- *Rejection*: If the Chief Privacy Officer and/or Chief Information Security Officer, or their designees, in consultation with the Chief Operating Officer and the Office of the County Counsel, deem that a department's training content or training requirements are not adequate, then that department's employees must take the trainings required by this policy.

Definitions

None.

Frequently Asked Questions

1) **Do these training courses provide general or role-based training in information privacy and cyber security?**

This policy refers to general introductory-level information privacy training and cyber security training. If a department desires additional role-based training, the department may contact the Privacy Office and/or the Information Security Office to discuss the possible development of such training.

2) **Is this training a requirement or a suggestion, and who does it apply to at the County?**

Information privacy training and cyber security training are requirements that apply to all employees, unless they are exempted by this policy. Employees must complete both training courses annually. If a department has equivalent privacy training and/or cyber security training and receives an exemption from the Privacy Office and/or Information Security Office, then that department's employees do not need to take the trainings required by this policy. See FAQ 3 for employees required to take HIPAA privacy and security training.

3) **If I am required to take HIPAA privacy and security training, am I also required to complete the additional privacy training and cyber security training required by this policy?**

No, employees who take HIPAA privacy and security training are not required to take the trainings required by this policy unless their

department requires them to do so, in addition to the HIPAA privacy and security training.

4) **Do other types of privacy training and cyber security training meet the requirements of this policy?**

The only training that meets the requirements of this Policy are (a) the County's introductory-level "Information Privacy Training" and "Cyber Security Training"; (b) HIPAA privacy and security training; or (c) a departmental-specific training pre-approved by the Privacy Office (for privacy training) or Information Security Office (for security training).

5) **If I have an employee who completes this training through means other than through the County's online training platform (i.e., virtual, in-person, paper-based), what do I need to do to keep track of and report training completion results?**

For employees completing the training in an alternative format, the department shall report within 90 days the completion results to the administrators of the online training platform.

Related Policies

- Board Policy 3.25 - Policy Relating to Confidentiality of Documents - https://saecommon.sccgov.org/countypolicy/Board-Policy-3.25-Policy-Relating-to-Confidentiality-of-Documents.pdf
- Incident Response Plan
- Notification of Security Breach of Personal Information - https://saecommon.sccgov.org/countypolicy/Notification-of-Security-Breach-of-Personal-Information.pdf

- Notification of Major or Sensitive Incidents (Incident Notification) - https://saecommon.sccgov.org/countypolicy/Incident-Notification.pdf

- Information Security Policies - https://saecommon.sccgov.org/countypolicy/Information-Technology-Security-Policies.pdf

- SCVHHS Department Policies - [url]/Pages/360compliancepolicies.pdf

Related Forms and Information

- Information Technology User Responsibility Statement - [url]/sites/policies/FormsrelatedtoPolicies/IT-User-Responsibility-Statement.pdf

- Notice of Data Breach Template - [url]/sites/policies/FormsrelatedtoPolicies/Notice-of-Data-Breach-Template.docx

History

Date	Changes Made
12/9/2021	Policy Adopted
12/14/2021	Policy Uploaded