Lake County Policy	*5.2 Cyber Security Awareness Training Policy*
	Approved by the County Board on: **August 12, 2025**

1. Purpose and Intent

1.1 The purpose and intent of the Cyber Security Awareness Training Policy is to establish a Lake County training program and guidelines to reduce the risk and impact from cyber security threats by educating employees on their role in combatting information security threats.

2. Background

2.1 Lake County seeks to protect its Information Technology (IT) infrastructure and the data that is in the County's IT network.

2.2 The Illinois Information Security Improvement Act (20 ILCS 1375) requires that "Every employee of a County or municipality shall annually complete a cybersecurity training program. The training shall include, but need not be limited to, detecting phishing scams, preventing spyware infections and identity theft, and preventing and responding to data breaches."

2.3 This policy is intended to comply with applicable state and federal laws and is based on relevant cyber security guidance.

3. Scope

3.1 This policy applies to all County employees in departments supervised by the County Administrator, employees that fall under the authority of the Lake County Board's Employee Policies and Procedures Manual, and all individuals who have access to the County network or information technology systems. (For example: employees of elected offices, contractors, consultants, vendors, interns, student workers, and temporary employees.)

3.2 This policy shall be interpreted consistent with and subject to applicable law. It supersedes all previous policies and/or memoranda that may have been issued on subjects covered in this policy. Should any provision in this policy conflict with a specific provision in any other Board approved policy, the provisions in this policy shall take precedence.

3.3 This policy is not intended to supersede or limit the County from enforcing programs or provisions in any applicable collective bargaining agreement.

4. Authority

4.1 The County Administrator through the Chief Information Officer (CIO) is directed and has the authority to establish, maintain, and enforce a County-wide cyber security awareness training program.

4.2 The County Administrator is authorized to develop and issue directives and procedures for the effective implementation and enforcement of this policy and to adapt to changing

circumstances and business needs, consistent with County's commitment to maintaining cyber security.

4.3 Department, office, and commission leadership must ensure compliance with this policy, but have the authority to require additional cyber security training, not to conflict or replace the training directed by the County Administrator through the CIO.

5. Policy

5.1 The County-wide cyber security awareness training program shall include:

5.1.1 Initial cyber security awareness training to be completed during onboarding before access to the County network is allowed.

5.1.2 All County employees are required to complete annual cyber security training that shall be completed within 30 days of delivery.

5.1.3 Additional monthly cyber security training will be provided, and participation is highly encouraged.

5.1.4 Additional cyber security awareness training as required to address new threats, vulnerabilities, and individual staff training/testing performance.

5.1.5 Periodic evaluation actions (phishing emails, etc.) to evaluate overall effectiveness of the training.

5.1.6 Regular published reports to department, commission, and office leadership showing compliance and completion rates.

5.1.7 Regular published reports to the County Administrator showing overall, Countywide compliance and completion rates.

5.2 Compliance.

5.2.1 Failure to complete annual cyber security awareness training provided by the CIO and Enterprise IT Department will be considered a violation of this policy.

5.2.2 Repeated phish testing failures will be considered a violation of this policy.

5.2.3 Any employee or individual who has access to the Lake County network and fails to comply with this policy will be subject to discipline up to and including removal of access to the network and termination.

5.2.4 Exceptions to this policy can be made by the CIO and County Administrator.

5.3 Policy Review and Update.

5.3.1 The County Administrator through the CIO shall review this policy according to 1.1 Policy on Policy Making Framework.

5.3.2 Any modifications to this policy will be provided to the Lake County Board according to 1.1 Policy on Policy Making Framework.

6. Severability

6.1 If any section or provision of this policy should be held invalid by operation of law, none of the

remainder shall be affected.

7. Non-Discrimination

7.1 Lake County prohibits the discriminatory application, implementation, or enforcement of any provision of this policy on the basis of race, color, sex, age, religion, disability, national origin, ancestry, sexual orientation, marital status, parental status, military discharge status, source of income, gender identity, housing status, or any other protected category established by law, statute, or ordinance.

Policy History			
Version	**Date Adopted**	**Legistar Item #**	**Notes**
Original	March 14, 2023	23-0396	--
Amended	August 12, 2025	25-0981	Amended to reference state statute, required annual training, encouraged monthly training, and various clarifications.