RESOLUTION NO. 2026 R-_____ **SEMINOLE COUNTY, FLORIDA**

RESOLUTION

of the

SEMINOLE COUNTY BOARD OF COUNTY COMMISSIONERS

AMENDING THE SEMINOLE COUNTY ADMINISTRATIVE CODE BY RETITLING SECTION 26.5 FROM "INFORMATION SECURITY/DATA ACCESS POLICY" TO "INFORMATION SECURITY AND ARTIFICIAL INTELLIGENCE POLICY", AMENDING THE PURPOSE AND SCOPE SUBSECTIONS, ADDING A GENERAL SUBSECTION, ADDING AN ARTIFICIAL INTELLIGENCE SUBSECTION, AMENDING THE TRAINING SUBSECTION, DELETING THE "ROLES" AND "DIRECTIVES" SUBSECTIONS, AMENDING THE "NON-COMPLIANCE" SUBSECTION, DELETING THE "RESPONSIBILITY" SUBSECTION; AND PROVIDING AN EFFECTIVE DATE.

WHEREAS, Seminole County Ordinance No. 89-28 created the Seminole County Administrative Code; and

WHEREAS, Seminole County Resolution Numbers 89-R-438 and 05-R-151 adopted the Seminole County Administrative Code; and

WHEREAS, the Seminole County Administrative Code needs to be amended from time to time to reflect changes in the administration of County government; and

WHEREAS, Seminole County has determined that certain updates, including the need to retitle, reorganize, eliminate redundancy, remove outdated sections or language, and update outdated sections or language are necessary for clarity, to increase efficiency, and for ease of administration; and

WHEREAS, the "Purpose", "Scope", and "Non-Compliance" subsections are revised for brevity and technical accuracy; and

WHEREAS, the "General" subsection added to clarify certain roles and responsibilities, provide administrative directive on use of County-owned devices, ownership of data, procurement

of goods and services involving technology, and the reporting of incidents and suspicious information to the Information Technology Security Team; and

WHEREAS, an "Artificial Intelligence ("AI")" subsection is added to explain AI and provide for acceptable and unacceptable uses of AI; and

WHEREAS, the "Training" subsection is amended to comply with Section 282.3185, Florida Statutes; and

WHEREAS, the "Roles", "Directives", and "Responsibility" subsections are deleted and, to the extent necessary, consolidated into the "General" subsection; and

WHEREAS, Section 26.5 of the Seminole County Administrative Code is amended as set forth in the attached Exhibit A; and

WHEREAS, the Seminole County Board of County Commissioners have a public purpose in the efficient administration of information technology matters of Seminole County government.

NOW, THEREFORE, BE IT RESOLVED, by the Board of County Commissioners of Seminole County, Florida that:

Section 1. Section 26.5 of the Seminole County Administrative Code is hereby amended by the new Section 26.5, as set forth in Exhibit A, attached hereto and made part of this Resolution.

Section 2. This Resolution and the attached Exhibit A will take effect immediately following their adoption and will remain in effect until terminated or superseded by further action of the Board.

[The remainder of this page has been left blank.]

ADOPTED this _____ day of _____, 2026.

ATTEST:

BOARD OF COUNTY COMMISSIONERS
SEMINOLE COUNTY, FLORIDA

_____

By: _____
ANDRIA HERR, Chairman

GRANT MALOY
Clerk to the Board of
County Commissioners of
Seminole County, Florida.

Date: _____

Attachments:
Exhibit A: Section 26.5 (clean)

BP/
9/16/25

SECTION 26. INFORMATION ~~SERVICES~~ TECHNOLOGY DEPARTMENT

26.5 INFORMATION SECURITY/~~DATA ACCESS~~ AND ARTIFICIAL INTELLIGENCE POLICY

A. PURPOSE.

~~(1)~~ The purpose of ~~the~~ this Information Security/~~Data Access~~ and Artificial Intelligence Policy ("Policy") is to ~~provide direction for effectively and efficiently managing the~~ establish security standards and procedures, manage informational technology related risks, protect ~~to~~ Seminole County the "County" ~~Government's~~ information technology assets, and ensure data availability, confidentiality, and integrity. ~~against accidental or malicious disclosure, modification or destruction whether internal or external, deliberate, or accidental.~~

~~(2) Security is critical to the organization's survival. This policy also defines the access controls that must be put into place to protect information by controlling who has the right to access the information assets, whether it is actual data, the hardware on which the data resides, or the application software used to manipulate data on systems installed throughout the County.~~

B. SCOPE. This ~~p~~Policy applies to all ~~members of the Board of County Commissioners, its departments, employees, volunteers, interns, contractual third parties, appointed committee members and Seminole County Constitutional Officers and their employees~~ individuals with any form of access to the ~~information and~~ information technology systems ~~which impact the daily operations of~~ ~~Seminole~~ the County ("Users") ~~Government~~.

C. GENERAL.

(1) The Chief Information Officer ("CIO") is designated as the Chief Information Security Officer ("CISO") for the County. The CIO is responsible for providing governance, management, and oversight to the Information Technology Department and the CIO and their designees are responsible for establishing County-wide standards and procedures as it relates to technology, artificial intelligence ("AI"), and data, including but not limited to, approved platforms, administrative access rights, extent of access control, and password management.

(2) In coordination with and as approved by the CIO, the Information Security Division Manager ("ISDM") is responsible for maintaining and executing information security frameworks, developing security standards and procedures, establishing and maintaining security incident response plans, and providing outreach and cybersecurity training for County employees.

(3) All Users utilizing County-owned devices, including but not limited to, cellphones, tablets, and laptops ("Devices"), must do so in accordance with all applicable State of Florida and Federal laws, rules, regulations, and County policies. Users may only utilize County Devices for County business. Users are responsible for activities conducted using County-owned Devices within the reasonable control of the User and may not

attempt to circumvent or modify the security features and non-administrative controls set forth by the Information Technology Department.

(4) Users must not share passcodes and passwords with any other individual, irrespective of whether another individual is a User.

(5) All data, including hardware and software, and Devices are owned by the County, some of which may be licensed or leased from a third-party or created by a User. If a User creates intellectual property using County data, which includes County information, that is not publicly available, whether during the course and scope of employment or thereafter, the intellectual property is owned solely by the County.

(6) Prior to any procurement containing technology in whole or in part, the user department must submit an IT Request Form to the assigned departmental project management team member within the Information Technology Department ("Project Manager"). The Project Manager will evaluate the request with other units within the Information Technology Department, such as the Security and Infrastructure teams, and the CIO, who must approve the request prior to soliciting the goods or services irrespective of the amount of the goods or services sought.

(7) Users must retain public records, as defined in Ch. 119, Florida Statutes, in accordance with the Public Records Maintenance, Storage, and Retention Policy set forth in the Seminole County Administrative Code.

(8) Users must immediately report incidents and suspicious information technology related activity to the Information Technology Security Team at: CSDSupport@SeminoleCountyFL.gov and InfoSec@SeminoleCountyFL.gov.

D. Artificial intelligence. AI is technology that enables computers and machines to simulate tasks performed by humans, such as learning, reasoning, comprehension, problem solving, and decision-making. AI technologies may include, but are not limited to, generative artificial intelligence tools, machine learning systems, predictive analytics technologies, automated decision-support systems, and vendor platforms that incorporate artificial intelligence capabilities. Generative AI creates new content, including text, images, code, audio, or video. For purposes of this Policy, AI and Generative AI are referred to as AI.

(1) **Acceptable Use and Requirements of AI.**

(A) Only those AI platforms approved by the CIO or their designees may be used for County business and only in accordance with all applicable State of Florida and Federal laws, rules, regulations, and County policies. When using AI platforms approved by the CIO or their designees, Users must independently verify all outputs through human review and may not solely rely on AI-generated content for accuracy, completeness, or decision-making.

(B) If Users intend to use data that is the subject of a contract or potential contract between the County and a third-party, Users must review the contract provisions to determine whether there are any prohibited uses of data in AI platforms. At all times, Users must comply with contract terms.

(C) If information or work product generated by AI is published publicly by a User, a statement must be included with the information or work product that it was generated with the use of AI.

(D) By using AI, Users acknowledge that AI is not error-free. The use of AI depends on data input and AI does not factor in human awareness. Therefore, Users must be aware of grammatical errors and incomplete results that may be produced. In all cases, AI results must be validated by Users.

(2) **Unacceptable Uses of AI.** Users must not input confidential information, including but not limited to, social security, credit card, cybersecurity, Health Insurance Portability and Accountability Act ("HIPPA"), or personally identifiable information, into AI platforms. Confidential information is information that is protected by any applicable law or may reasonably be determined to be sensitive. Instead, Users must anonymize or de-identify information prior to the use of AI.

~~C~~**E. TRAINING.** Cybersecurity training is a foundational component of protecting the County's information technology network and data from cyber threats and to ensure availability, confidentiality, and integrity. Pursuant to Section 282.3185, Florida Statutes, all local government employees and technology professionals must complete cybersecurity training within thirty (30) days after commencing employment and annually thereafter, to strengthen awareness, reduce risks, and improve response capabilities. The mandatory training, including simulated phishing exercises, will be established by the Information Technology Department.

~~(1) Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information, information systems or both.~~

~~(2) It is the responsibility of every computer user to know what constitutes acceptable use of Seminole County Government systems, to know the guidelines, and to conduct their activities accordingly.~~

~~(3) All employees and third-party vendors shall receive training and supporting reference materials to allow them to properly protect Seminole County Government information assets before they are granted access.~~

~~(4) Security awareness training will be provided at regular intervals to ensure that all necessary employees maintain the desired level of proficiency.~~

~~**D. ROLES.** The roles of specific County staff in implementing this policy are set forth below:~~

~~(1) Data Custodian: A member or members, who have ultimate responsibility for ensuring the protection and use of the organization's data. Responsibilities include:~~

~~(a) Identifying what data belongs to the Board and identifying the system of record.~~

~~(b) Identifying and documenting what roles are allowed access to the data and the level of access required.~~

~~(c) Determining and documenting the process for authorizing individuals to access the data.~~

~~(d) Implementing processes that maintain the integrity and accuracy of the data.~~

~~(e) Ensuring that the data is protected, and the applicable laws are followed concerning handling of the data.~~

~~(2) Security Administrator: This role is responsible for the security of the data and systems that store the data. The responsibilities of this role include:~~

~~(a) Providing access to the users that are approved by the data custodian.~~

~~(b) Protecting data from unauthorized users.~~

~~(c) Ensuring that appropriate disaster recovery procedures are in place.~~

~~(3) Data User: The role is designated by the data custodian and has permission to access and use the data. Responsibilities include:~~

~~(a) Being accountable for all data made with his or her account.~~

~~(b) Ensuring that all use and distribution of data is only for approved purposes.~~

~~(c) Not disclosing data to unauthorized people.~~

~~(d) Keeping his or her password secret.~~

~~(4) Information Security Officer: This role is designated by the Chief Information Officer and responsibilities include:~~

~~(a) Assuming overall responsibility for the security of the County's information systems and data integrity.~~

~~(b) Establishing the policies and procedures necessary to ensure the security and integrity of the County's data and information systems.~~

~~(c) Working with Data Custodians to ensure the reliability and enforcement of any related policies and procedures.~~

~~(d) Organizing incident response to security breaches in order to minimize data loss or integrity concerns.~~

~~(5) Information Services Department: This role is responsible for supporting the electronic data systems infrastructure. Responsibilities include:~~

~~(a) Documenting and supporting the structure of the organization's data.~~

~~(b) Supporting the use of standard data definitions throughout the organization.~~

(c) Facilitating the appropriate sharing of data and integration of data between the organization's systems.

(6) Chief Information Officer: This role is responsible for providing oversight to the Information Services Department and providing guidance to the county on information systems issues. Responsibilities include:

(a) Appointing and revoking Data Custodian roles to all electronic information systems.

(b) Assuming the role of Information Security Officer in absence of other designees.

E. DIRECTIVES.

(1) All data, including software, produced by County employees, volunteers, interns, Commissioners and their aides, and third-party vendors while employed by the Board, is solely owned by the Seminole County Board of County Commissioners.

(2) All computer hardware, computing devices, including tablets and smart phones, operating systems, and third-party software applications purchased using funding provided by the Board are solely owned by the Seminole County Board of County Commissioners.

(3) Access to any information system that has security risks requires authentication by userid or password, biometric system, multi-factor authentication or other mechanism which minimizes unauthorized access to or alteration of the County's data. The Information Security Officer shall approve the appropriate authentication method.

(4) The Information Security Officer shall document and maintain appropriate standards for the creation, size, style and expiration period of passwords. All data users shall follow the standards.

(5) The Board delegates the responsibility for ensuring that the appropriate level of user access management is implemented and maintained in a secure manner to the Chief Information Officer or his or her designees. The Chief Information Officer shall assign an appropriate Data Custodian for each of the computer systems owned by the Board of County Commissioners.

(6) Formal user access control procedures must be documented, implemented and kept up to date by the Data Custodian for each application and information system to ensure authorized user access only. These procedures must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Security Administrators shall allocate access rights and permissions for each user to computer systems and data that are commensurate with the task they are expected to perform. Users will not be granted access to information that is unnecessary for the performance of their tasks. The system's Data Custodian is responsible for determining the appropriate authorization levels for each data user.

~~(7) Where Board owned data systems cross the boundaries of the Board and other Constitutional Officers, the Chief Information Officer shall create a committee composed of members of both organizations to ensure that the data integrity and operational needs of both organizations are met. The Board of County Commissioners shall resolve any disputes. Under any circumstance, the Board delegates to the County Manager the ability to request access rights to any Board owned system for any data user. Any request made by the County Manager must be fulfilled as soon as possible.~~

~~(8) Employees outside the Information Services Department do not have administrative rights to any of the Board's information systems unless that access is granted in writing by the County Manager, Chief Information Officer, or designee(s).~~

~~(9) No information created by an employee of the Board of County Commissioners that is produced using County equipment will be considered private to the employee.~~

~~(10) Employees shall not install software on their computers or any computing device without the approval of the Information Security Officer or his or her designee.~~

~~(11) All employees of the Board of County Commissioners must retain data as required by Chapter 119, Florida Statutes (2016), as this statute may be amended from time to time ("Public Records"), and all other applicable law. Under no circumstance may an employee release data to the general public that is exempt from Chapter 119, Florida Statutes (2016), as this statute may be amended from time to time, and all other applicable law.~~

F. NON-COMPLIANCE. ~~Non-compliance~~ Failure to comply with this Policy ~~by Seminole County employees and system users is a serious matter and will be dealt with accordingly on a case-by-case basis. Depending on the severity of violations and applicable legal statutes, consequences could~~ may result in removal or limitation of access rights ~~and special system privileges, removal of system access,~~ or~~, for County employees,~~ disciplinary action~~, to include~~ including but not limited to, potential termination of employment. ~~In severe cases of fraud or breach of privacy laws, legal action may be taken.~~

~~**G. RESPONSIBILITY.** The Board of County Commissioners bears the ultimate authority and responsibility for Seminole County Government's information security. As such, the Board has established this Policy and directs Seminole County Government personnel to implement the Information Security/Data Access Policy as follows:~~

~~(1) The County Manager shall approve and enforce all information security guidelines that have county-wide scope.~~

~~(2) The County Manager shall appoint the Chief Information Officer or his or her designee as the Information Security Officer (ISO) to provide the direction and technical expertise to ensure that Seminole County Government's information is properly protected.~~

~~(3) All Seminole County Government Directors, Managers, Program Managers, Supervisors and other Seminole County Constitutional Officers (where their staff access~~

~~the County's data systems) are directly responsible for implementing the Information Security/Data Access Policy and any subsequent policies, procedures and guidelines developed by the Information Security Officer and approved by the County Manager within their areas of responsibility, and for adherence by their staff.~~

~~H~~ G. AUTHORITY. ~~Public Records Act, Chapter 119, Florida Statutes~~
Resolution 2003-R-36 adopted February 11, 2003
Resolution 2007-R-42 adopted March 13, 2007
Resolution 2008-R-55 adopted February 12, 2008
Resolution 2010-R-26 adopted January 26, 2010
Resolution 2012-R-107 adopted June 12, 2012
Resolution 2016-R-187 adopted November 15, 2016
Resolution 2026-R- adopted