INDIAN RIVER COUNTY, FLORIDA

MEMORANDUM

Departmental

TO: Indian River County Board of County Commissioners

VIA: Michael Zito, Interim County Administrator

FROM: Dan Russell, Information Technology Director

SUBJECT: Information Technology Policy Additions to the Administrative Policy Manual

DATE: January 31, 2023

BACKGROUND:

The recent enactment of section 282.3185, Florida Statutes, (Local Government cybersecurity) requires local governments to adopt cybersecurity standards that safeguard their data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Each county with a population of 75,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Furthermore, each local government shall notify the Florida Digital Service of its compliance with this subsection as soon as possible.

The Indian River County Information Technology Department has been pursuing alignment with the best practices outlined in the NIST CSF for the past several years. Over the course of the past year the IT Department has created a requirements trace matrix for all of the security controls specified by the NIST CSF and mapped those security controls that require the creation of an organizational policy into the twenty one policies listed below. To comply with section282.3185, Florida Statutes, the Information Technology Department is recommending the following Information Technology and Cybersecurity policy additions to the Administrative Policy Manual (APM):

- AM-1200.01 - Contingency Planning
- AM-1200.02 - Incident Response
- AM-1200.03 - Awareness and Training
- AM-1200.04 - Program Management
- AM-1200.05 – Planning
- AM-1200.06 - Identification and Authentication
- AM-1200.07 - System and Communications Protection
- AM-1200.08 - Configuration Management
- AM-1200.09 - Access Control
- AM-1200.10 - Audit and Accountability
- AM-1200.11 - Assessment, Authorization, and Monitoring
- AM-1200.12 - Maintenance
- AM-1200.13 - System and Information Integrity
- AM-1200.14 - Media Protection
- AM-1200.15 - Physical and Environmental Protection
- AM-1200.16 - Personnel Security
- AM-1200.17 - System and Services Acquisition
- AM-1200.18 - Risk Assessment
- AM-1200.19 - Supply Chain Risk Management
- AM-1200.20 - Personally Identifiable Information Processing and Transparency

- AM-1200.21 - Acceptable Use

FUNDING

There is no funding requirement associated with the addition of these policies to the APM. However, proper implementation and sustainment of these policies may result in future request for additional funding.

RECOMMENDATION

Staff recommends that the Board approve the addition these policies to the APM.

ATTACHMENTS

AM-1200.01 - Contingency Planning
AM-1200.02 - Incident Response
AM-1200.03 - Awareness and Training
AM-1200.04 - Program Management
AM-1200.05 – Planning
AM-1200.06 - Identification and Authentication
AM-1200.07 - System and Communications Protection
AM-1200.08 - Configuration Management
AM-1200.09 - Access Control
AM-1200.10 - Audit and Accountability
AM-1200.11 - Assessment, Authorization, and Monitoring
AM-1200.12 - Maintenance
AM-1200.13 - System and Information Integrity
AM-1200.14 - Media Protection
AM-1200.15 - Physical and Environmental Protection
AM-1200.16 - Personnel Security
AM-1200.17 - System and Services Acquisition
AM-1200.18- Risk Assessment
AM-1200.19 - Supply Chain Risk Management
AM-1200.20 - Personally Identifiable Information Processing and Transparency
AM-1200.21 - Acceptable Use

DISTRIBUTION

Dylan Reingold – County Attorney
IRC BoCC Department Heads