

TO: ALL COUNTY PERSONNEL

FROM: VERDENIA C. BAKER
COUNTY ADMINISTRATOR

PREPARED BY: INFORMATION SYSTEMS SERVICES DEPARTMENT (ISS)

SUBJECT: CYBERSECURITY AWARENESS TRAINING FOR EMPLOYEES
AND OFFICIALS

PPM #: CW-P-085

=====

ISSUE DATE
June 14, 2024

=====

=====

EFFECTIVE DATE
June 14, 2024

=====

PURPOSE:

To establish a cybersecurity awareness training requirement for all county employees and all Officials as defined below who access email, the internet or business applications from the county's enterprise network.

UPDATES:

Future updates to this PPM are the responsibility the Chief Information Officer (CIO).

AUTHORITY:

- Florida Statutes (F.S.), Section 282.3185, as may be amended
- PPM # CW-O-059 – Information Technology Security Policies, as may be amended

DEFINITIONS:

Employee: a person defined under F.S. 447.203, Fair Labor Standards Act. 29 U.S.C.A. 203, who performs services for and is under the control and direction of the Board of County Commissioners (BCC) for wages or other remuneration.

Enterprise Network: includes both the physical (wired) network and the wireless network managed by ISS or by any county agency managing physical access to the internet.

ISS Managed Departments: departments that utilize ISS services for user administration, email, business application development and support, desktop support, and various other IT-related services.

Officials: members of the BCC, and members appointed by the BCC who will access email or the

internet from the county's enterprise network.

Phishing: a process where people receive an email, instant messages or some other messaging service that looks to have come from a known contact or a reputable organization when in fact it is from a cybercriminal. These types of attacks have no specific targets sending out emails or messages in mass hoping someone responds back with personal information or that they click on a link or attachment within the email that installs malware on their computer.

Self-Managed Departments: departments that provide their own support for desktops, printers, servers, and department-specific business applications.

Simulated Phishing Campaigns: controlled tests of an employee's cybersecurity awareness by sending a simulated phishing email to select employees and monitoring their actions to determine whether they have fallen victim to the simulated phishing attack, whereupon feedback will be provided to the employee for their awareness and training.

BACKGROUND:

Palm Beach County relies heavily upon computer-based automation with most employees accessing email, the internet, and a multitude of business applications on a daily basis. Cyber criminals are aware of this and are increasingly targeting governmental organizations that do not have the resources to provide adequate cybersecurity awareness training, or to implement effective perimeter defenses. Studies show the weakest link in cyber defenses are the employees themselves. Therefore it is essential that all Officials and county employees have sufficient training to recognize cyber-attacks and understand best practices for IT security.

POLICY:

All officials and county employees, who require access to the County network, email, or enterprise business application must complete annual cybersecurity awareness training. In addition, staff must be aware of their responsibility for protecting county assets by maintaining cybersecurity awareness at all times while on the county's network.

All new Officials and newly hired county employees who will be granted access to the enterprise network will be scheduled for a series of mandatory cybersecurity awareness training courses offered by ISS within 30 days of their hire date. ISS will monitor those scheduled for mandatory training to ensure adherence to this PPM.

PROCEDURES:

Training

ISS will maintain a software subscription from a third party that provides a Learning Management System (LMS) for cybersecurity awareness training with a variety of course selections, along with reinforcement training for continuous improvement. The subscription will also support simulated phishing campaigns to measure training effectiveness.

Annual and new employee cybersecurity trainings will be scheduled by ISS to ensure compliance with applicable laws and policies.

Additional cybersecurity awareness training will be scheduled periodically for all enterprise network users as a means of reinforcing the importance of remaining vigilant when reading email and accessing the internet. This training will be optional and taken upon supervisor approval.

Phishing Campaign

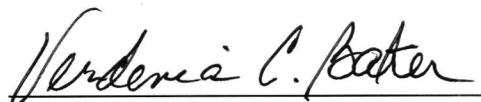
ISS will conduct simulated phishing campaigns to identify staff who fail to recognize emails containing malicious content. ISS will contact the employee's immediate supervisor to inform them when they have fallen victim twice and let them know the employee will be assigned additional mandatory training.

ISS Managed Departments

1. ISS will setup all existing employees in the LMS and develop a process for adding new employees and removing terminated employees.
2. A series of cybersecurity awareness courses will be scheduled annually and/or within 30 days of employment for all Officials and county employees. Random simulated phishing campaigns will be scheduled once training is complete to measure training effectiveness and for continual reinforcement. Those who fall victim twice will be scheduled for further mandatory training.
3. Additional optional training will be scheduled periodically for continual reinforcement, or to highlight a current threat that may be occurring around the world.
4. A specialized training curriculum can be designed for employees whose job functions require handling of HIPAA information and/or for those who process credit cards.

Self-Managed Departments

ISS will provide administrative access to the LMS for self-managed agencies who choose to schedule and manage training on their own.


VERDENIA C. BAKER
COUNTY ADMINISTRATOR

Supersession History:

1. PPM# CW-P-085, effective March 8, 2018