OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

John A. Carey
Inspector General

Inspector General
Accredited

"Enhancing Public Trust in Government"

Audit Report

2023-A-0001

Town of Highland Beach - IT Network Security Review

November 21, 2022

Insight – Oversight – Foresight

Office of Inspector General
Palm Beach County

Audit Report
2023-A-0001

John A. Carey
Inspector General

Date Issued: November 21, 2022

Inspector General
Accredited

"Enhancing Public Trust in Government"

Town of Highland Beach - IT Network Security Review

SUMMARY

WHAT WE DID

We conducted an Information Technology (IT) Network Security review of the Town of Highland Beach (Town).[1] This review was performed as part of the Office of Inspector General (OIG), Palm Beach County 2022 Audit Plan.

Our review focused on IT network security records and activities related to network components, such as devices, systems and data, in place during FY 2022.

WHAT WE FOUND

We found that the Town had processes in place designed to prevent network security intrusions; monitor and detect network security threats, breaches, and intrusions; and respond to network security threats, breaches, and intrusions.

However, the Town lacked sufficient written guidance for: (a) data and asset/component sanitization and disposal; (b) organizational cybersecurity processes, including incident response and contingency/recovery processes; and, (c) access control management.

WHAT WE RECOMMEND

Our report contains three (3) findings and eight (8) recommendations. Implementation of the recommendations will assist the Town in strengthening internal controls over IT Network Security.

The Town concurred and accepted the recommendations.

We have included the Town's management response as Attachment 1.

[1] This was a standard, non-technical, compliance-type review where we verified the existence of some basic IT network security practices and controls. Therefore, this review does not preclude the need for professional expertise and more comprehensive or in-depth assurance or advisory services, such as IT risk assessments, audits, and penetration testing.

BACKGROUND

The Town was created in 1949 by twenty-one voting residents as a water district. Because of saltwater intrusion in the Town's wells and the inability to connect with neighboring towns for fresh water, the residents formed a town and raised funds to build a water plant. The Town is bounded by the City of Delray Beach to the north and northwest and by the City of Boca Raton to the south and south west. Based on 2020 Census Data, the Town's 2020 population was approximately 4,295.[2]

The current Town Charter was adopted on January 7, 2003 by Town Ordinance No. 701. The Town provides general municipal services such as police protection and a library, as well as water and wastewater utility service. The Town also provides, through contract, fire protection, code enforcement, building inspection, solid waste and postal services.

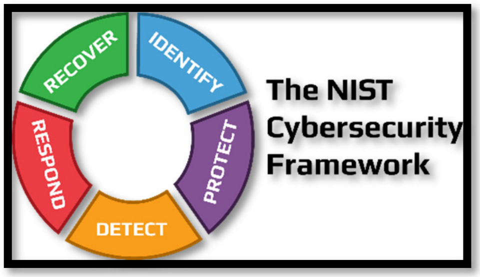
The government of the Town is vested in the Town Commission, which is composed of five (5) members elected to staggered three (3) year terms, one of whom is the elected Mayor-Commissioner and another is the elected Vice Mayor-Commissioner. The Town Commission appoints the Town Manager, who is the chief administrative officer.

The OIG FY 2022 Annual Audit Plan included IT Network Security Reviews. The Town of Highland Beach was selected for review because it has not been previously reviewed or audited by the OIG and because it operates a water utility, which increases the Town's IT Network Security risk.

OIG IT NETWORK SECURITY REVIEW CHECKLIST

NIST Framework

The National Institute of Standards and Technology (NIST) created a cybersecurity risk framework for use by critical infrastructure owners and operators. The NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Framework) Core consists of five interrelated functions:



- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

[2] http://edr.state.fl.us/Content/area-profiles/2020-census-county-city/2020PL94-171_099.pdf

- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

NIST Security and Privacy Controls

The NIST Security and Privacy Controls publication[3] establishes controls for systems and organizations that process, store, or transmit information. The publication was designed to help organizations identify the controls necessary to manage security and privacy risk and is intended to be used by a diverse audience, including, but not limited to:

- Individuals with system, information security, privacy, or risk management and oversight responsibilities, including authorizing officials, chief information officers, senior agency information security officers, and senior agency officials for privacy;

...

- Individuals with logistical or disposition-related responsibilities, including program managers, procurement officials, system integrators, and property managers;

...

- Individuals with security and privacy implementation and operations responsibilities, including mission or business owners, system owners, information owners or stewards, system administrators, continuity planners, and system security or privacy officers;

...

- Individuals with security and privacy assessment and monitoring responsibilities, including auditors, Inspectors General, system evaluators, control assessors, independent verifiers and validators, and analysts.

The NIST Security and Privacy Controls includes, but is not limited to the following control groups:

- Access Control
- Audit and Accountability
- Identification and Authentication
- Media Protection
- Awareness and Training
- Contingency Planning
- Incident Response
- Risk Assessment
- Personally Identifiable Information Processing and Transparency

[3] NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations

CIS Critical Security Controls

The Center for Internet Security (CIS)[4] Critical Security Controls publication was developed to assist organizations with focusing their efforts on defending themselves against cybersecurity attacks. Critical Security Controls were advanced by combining the knowledge of subject matter experts in the public and private sectors. An organization can integrate Critical Security Controls commensurate with its IT maturity.

Implementation Guidance (IG) 1 controls

IG 1 controls are suited for small to medium-sized organizations with limited IT and cybersecurity expertise dedicated to protecting IT assets and personnel. These controls focus on thwarting general, non-target attacks and are designed to work in conjunction with commercial off-the-shelf hardware and software. IG1 control groups include:

- Inventory and Control of Enterprise Assets
- Inventory and Control of Software Assets
- Secure Configuration of Enterprise Assets and Software
- Data Protection
- Account Management
- Access Control Management
- Continuous Vulnerability Management
- Audit Log Management
- Email and Web Browser Protections
- Malware Defenses
- Data Recovery
- Network Infrastructure Management
- Security Awareness and Skills Training
- Service Provider Management
- Incident Response Management

IG 2 controls

IG 2 controls are suited for enterprises employing individuals who are responsible for managing and protecting IT infrastructure. Often these organizations have regulatory burdens related to processing and storing sensitive customer information. These controls help security teams manage operational complexity. In addition to the IG 1 control groups, IG 2 control groups include:

- Network Monitoring and Defense
- Application Software Security
- Penetration Testing

[4] The Center for Internet Security (CIS) is a community-driven 501(c)(3) nonprofit organization, formed in October 2000. Its mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against cyber threats. The organization is headquartered in East Greenbush, New York, with members including large corporations, government agencies, and academic institutions. https://www.cisecurity.org/about-us

IG 3 controls

IG 3 controls are suited for enterprises that employ security experts that specialize in cybersecurity risk management, penetration testing, and application security. IG 3 controls strengthen the IG 1 and IG 2 control groups in an effort to mitigate targeted attacks from sophisticated adversaries.

IT Network Security Review Checklist

We developed an IT Network Security Review checklist of cybersecurity activities and controls centered on the NIST Framework Core, which is a set of cybersecurity activities, desired outcomes, and references that are common across critical infrastructure sectors. The IT Network Security Review checklist focuses on activities and controls recommended in the NIST Special Publication 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations (Security and Privacy Controls), the use of which is mandatory for federal information systems, and the CIS Critical Security Controls (Version 8) IG 1,[5] which are considered "essential cyber hygiene" that can be implemented with limited cybersecurity expertise aimed to thwart general, non-targeted attacks.

We developed our IT Network Security Review checklist to include activities and controls related to:

- Physical Devices (Hardware),
- Account Management (User and Administrative),
- Organizational Cybersecurity Policy,
- Access Control Management,
- Disposition of Data,
- Malware Defenses,
- Email and Web Browser Protections,
- Network Security Awareness Program and Training,
- Incident Management Response Plan, and
- Contingency/Recovery Planning.

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objectives of the review were to determine whether the Town had processes in place designed to:

1) Prevent network security intrusions;
2) Monitor and detect network security threats, breaches, and intrusions; and
3) Respond to and eliminate network security threats, breaches, and intrusions.

The scope of the review was limited to IT network security records and activities related to significant IT network components, such as devices, systems, and data, in place during FY 2022.

[5] https://www.cisecurity.org/controls

The review methodology included but was not limited to:

- Reviewing ordinances, policies, procedures, and related requirements;
- Conducting a review of IT Network Security processes and controls based on the NIST Framework for Improving Critical Infrastructure Cybersecurity and the CIS Critical Security Controls;
- Interviewing appropriate personnel; and
- Reviewing records, logs, and reports.

This review was conducted in accordance with the Principals and Standards for Offices of Inspector General. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

FINDING AND RECOMMENDATIONS

Finding (1): The Town lacked sufficient written guidance for data and asset/component sanitization and disposal.

The NIST Framework describes information protection processes and procedures as security policies, processes, and procedures that are used to manage the protection of information systems and assets. The NIST Security and Privacy Controls for information protection processes and procedures include having media and component sanitization and disposal processes and procedures. Additionally, the CIS Critical Security Controls IG1 includes data protection controls to securely dispose of data stored on the network, whether it is stored remotely or on enterprise assets and devices.

Data and asset/component sanitization and disposal controls include:

- Establish and maintain a data management process that addresses data retention limits and disposal requirements and ensures the disposal process and method is commensurate with the data sensitivity;
- Reviewing and approving assets to be sanitized to ensure compliance with record retention requirements;
- Tracking and documenting actions including listing personnel who reviewed and approved sanitization and disposal actions, types of assets sanitized, files stored on the asset, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitation, verification actions taken and personnel who performed the verification, and the disposal actions taken;
- Disposing of data, documentation, tools, or system components as outlined in the data management process;
- Remote purging or wiping of data on lost or stolen organizational assets;
- Verification that the sanitization of the asset was effective prior to disposal; and
- Testing of sanitation equipment and procedures.

We found that the Town had processes with controls to assist with data and asset/component sanitization and disposal; however, there were no written policies or procedures documenting the processes and controls in place.
The Assistant Town Manager stated there were no written policies and procedures providing guidance on data sanitization, asset/inventory item disposal, or reporting lost or stolen equipment. Moreover, Town staff explained that during the period between 2008 and 2019, there was consistent turnover in the Town Manager position, which led to a lack of organizational structure. As a result, many policies that were enacted or adopted were not updated, revised, or reviewed until the current Town Manager and the Commission adopted a strategic priorities plan that included updating policies and procedures.

The IT policies and procedures in place at the time of our review, and the IT Policy implemented during our review, which was effective as of August 1, 2022, did not include sufficient controls and written guidance related to the Town's data and asset/component sanitization and disposal process.

A lack of written policies and procedures for data and asset/component sanitization and disposal increases the risk associated with loss of control over protected or sensitive data.

Recommendations:

(1) The Town develop and implement written Data and Asset/Component Sanitization and Disposal policies and procedures that provide guidance regarding:

- **a. Data retention and disposal requirements and to ensure the disposal process and method are commensurate with the data sensitivity;**
- **b. Reviewing and approving assets to be sanitized to ensure compliance with record retention requirements;**
- **c. Tracking and documenting sanitization and disposal actions and approvals;**
- **d. Disposing of data, documentation, tools, or system components as outlined in the data management process;**
- **e. Remote purging or wiping of data on lost or stolen organizational assets;**
- **f. Verifying that the sanitization of the asset was effective prior to disposal; and,**
- **g. Testing of sanitation equipment and procedures.**

(2) The Town provide ongoing training to ensure staff are aware of their roles and responsibilities related to data and asset/component sanitization and disposal.

Management Response:

Management accepts the finding and recommendations. The Town will review the current IT policy and update as necessary to outline the process and procedures regarding data and asset/component sanitization and disposal. Additionally, upon

amending the IT policy, the Town will provide ongoing training to staff members to ensure they are aware of the roles and responsibilities as it relates to data and asset/component sanitization and disposal.

Finding (2): The Town lacked sufficient written guidance for the organizational cybersecurity process, including incident response and contingency/recovery processes.

The NIST Framework describes governance as the policies, procedures, and processes implemented by an organization to manage and monitor regulatory, legal, environmental, and operational requirements that inform management of cybersecurity risk. The NIST Security and Privacy Controls for Governance of cybersecurity include having a documented Incident Response Plan and a documented Contingency/Recovery Plan. Additionally, the CIS Critical Security Controls IG1 includes establishing an Incident Response Management program to develop and maintain incident response capability (e.g. policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack as well as a Data Recovery process to restore in-scope enterprise assets to a pre-incident and trusted state.

Incident Response Plan controls include:

- Designating one key person, and at least one backup, who will manage the incident handling process;
- Establishing and maintaining contact information for parties that need to be informed of security incidents;
- Establishing and maintaining a process to report security incidents; and,
- Tracking and documenting security incidents.

Contingency/Recovery Plan controls include:

- Identifying essential mission and business functions and associated contingency requirements;
- Identifying recovery objectives and restoration priorities;
- Addressing contingency roles, responsibilities, and assigned individuals with contact information;
- Addressing maintaining essential mission and business functions despite a system disruption, comprise, or failure; and,
- Addressing eventual, full system restoration without deterioration of the controls originally planned.

We found that the Town had processes with controls to assist with continuity of operations during a cybersecurity incident; however, the IT policies and procedures in place at the time of our review did not include sufficient controls and written guidance related to the Town's organizational cybersecurity processes, to include Incident Response and Contingency/Recovery plans.

The Assistant Town Manager stated there was no documented organizational cybersecurity policy, nor written policies and procedures providing guidance to employees related to either an Incident Response Plan or a Contingency/Recovery Plan; however, the Town was in the process of updating its IT Policy to include such guidance. The Assistant Town Manager stated that during the period between 2008 and 2019, there was consistent turnover in the Town Manager position, which led to a lack of organizational structure. As a result, many policies that were enacted or adopted were not updated, revised, or reviewed until the current Town Manager and the Commission adopted a strategic priorities plan that included updating policies and procedures.

Corrective Action

We reviewed the Town's IT Policy implemented during our review, which was effective as of August 1, 2022, and found it designated responsibilities for and established processes to manage and monitor cybersecurity risks, including an Incident Response Plan. However, it did not include a sufficient Contingency/Recovery plan because the policy did not provide recovery objectives, restoration priorities, and metrics; address contingency roles and responsibilities; assign individuals with contact information; address maintaining essential mission and business functions despite a system disruption, compromise, or failure (i.e. procedures and documentation while systems are not functioning); and address eventual, full system restoration without the deterioration of the controls originally planned and implemented.

A lack of sufficient written policies and procedures for the organizational cybersecurity processes, including incident response and contingency/recovery processes, increases the risk associated with identifying and responding to network threats and continuity of operations during and after a cybersecurity incident.

Recommendations:

(3) The Town implement a written IT policy that ensures cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners, and include governance and risk management processes addressing cybersecurity risks.

(4) The Town develop and implement a written Incident Response Plan policy and procedure to ensure continuity of operations that provide guidance including:

- **a. Designating one key person, and at least one backup, who will manage the incident handling process;**
- **b. Establishing and maintaining contact information for parties that need to be informed of security incidents, including where appropriate, law enforcement, government administrative agencies, and individuals whose information may have been compromised;**
- **c. Establishing and maintaining a process for staff to report security incidents; and,**
- **d. Tracking and documenting security incidents.**

(5) The Town develop and implement a written Contingency/Recovery Plan policy and procedure to ensure continuance of mission and business functions that provide guidance including:

a. Identifying essential mission and business functions and associated contingency requirements;

b. Identifying recovery objectives and restoration priorities;

c. Addressing contingency roles, responsibilities, and assigned individuals with contact information;

d. Addressing maintaining essential mission and business functions despite a system disruption, comprise, or failure; and,

e. Addressing eventual, full system restoration without deterioration of the controls originally planned.

(6) The Town provide ongoing training to ensure staff are aware of their roles and responsibilities in responding to and recovering from a network security incident, including maintaining business functions during a system disruption or failure.

Management Response:

Management accepts the findings and recommendations. The Town will review the current IT policy and update as necessary regarding cybersecurity roles and responsibilities to ensure they are coordinated and aligned with internal and external partners. The Town will update the written Incident Response Plan included in the current IT policy to identify key persons, contact information, outline the process for staff to report security incidents as well as how security incidents should be documented and tracked. The Town will additionally, develop and implement a written Contingency/Recovery Plan to be included in the current IT policy to ensure continuance of mission and business functions should a security incident occur. Lastly, the Town will implement ongoing training to ensure staff are aware of their roles and responsibilities in responding to and recovering from a network security incident.

Finding (3): The Town lacked sufficient written guidance for access control management.

The NIST Framework describes identity management and access control as ensuring access to physical and logical assets and associated facilities is limited to authorized users, processes and devices and is managed in accordance with the associated risk of unauthorized access to authorized devices and transactions. The NIST Security and Privacy Controls for access control management processes include having account management, access enforcement, separation of duties, least privilege[6], access control for mobile devices, and identification and authentication processes and procedures The CIS Critical Security Controls IG1 includes processes and tools to assign and manage

[6] Only the minimum necessary rights should be assigned to a subject that requests access to a resource and should be in effect for the shortest duration necessary.

authorization credentials as well as create, assign, manage, and revoke access credentials and privileges for user, administrative, and service accounts.

Account control management controls include:

- Establishing an account management process for assigning and managing user account authorizations
- Establishing an access granting process upon new hire, rights grant, or a role change;
- Establishing an access revoking process through disabling accounts immediately upon termination, rights revocation, or role change;
- Identifying, and dividing, business and support functions between different individuals, or roles, to reduce risk associated of authorized privileges abuse.
- Employing the principal of least privilege, allowing only authorized access for users that are necessary to accomplish assigned organizational tasks.
- Establishing configuration requirements, connection requirements and implementation guidance for mobile devices accessing the network.
- Establishing unique identification and authentication requirements (usernames, passwords, biometrics, etc.) for user accounts accessing the network.

We found that the Town had processes with controls to assist with granting and revoking user access to the network, maintaining role based control and documenting access rights for each role to carryout assigned duties, and employing the principal of least privilege, and we verified that only current employees had access to the network. However, there were no written policies or procedures documenting the processes and controls in place.

The Assistant Town Manager stated there were no written policies and procedures to assist with granting and revoking user access to the network, maintaining role based control and documenting access rights for each role to carryout assigned duties, and employing the principal of least privilege. Moreover, it was explained that during the period between 2008 and 2019, there was consistent turnover in the Town Manager position, which led to a lack of organizational structure. As a result, many policies that were enacted or adopted were not updated, revised, or reviewed until the current Town Manager and the Commission adopted a strategic priorities plan that included updating policies and procedures.

Corrective Action

We reviewed the Town's IT Policy implemented during our review, which was effective as of August 1, 2022, and found it includes guidance for assigning and managing user account authorizations; granting access upon new hire; limiting access based on roles/responsibilities; and, when necessary, revoking access. However, it did not include sufficient guidance for establishing configuration requirements, connection requirements and implementation guidance for mobile devices accessing the network.

A lack of written policies and procedures for access control management increases the risk for data breaches and unauthorized access and modification of enterprise systems and data because users have access to critical or sensitive data and systems that is not necessary to perform their roles and responsibilities within the organization.

Recommendations:

(7) The Town develop and implement a written access control management policy and procedure that provides guidance including:

a. Establishing an account management process for assigning and managing user account authorizations;

b. Establishing an access granting process upon new hire, rights grant or a role change;

c. Establishing an access revoking process through disabling accounts immediately upon termination, rights revocation, or role change;

d. Identifying, and dividing, business and support functions between different individuals, or roles, to reduce risk associated of authorized privileges abuse;

e. Employing the principal of least privilege, allowing only authorized access for users that are necessary to accomplish assigned organizational tasks;

f. Establishing configuration requirements, connection requirements and implementation guidance for mobile devices accessing the network; and,

g. Establishing unique identification and authentication requirements (usernames, passwords, biometrics, etc.) for user accounts accessing the network.

(8) The Town provide ongoing training to ensure staff are aware of their roles and responsibilities related to access control management.

Management Response:

Management accepts the findings and recommendations. The Town will review and update IT policy to provide a written procedure for access control management. Additionally, upon amending the IT policy, the Town will provide ongoing training to staff members to ensure they are aware of the roles and responsibilities as it relates to access control management.

ACKNOWLEDGEMENT

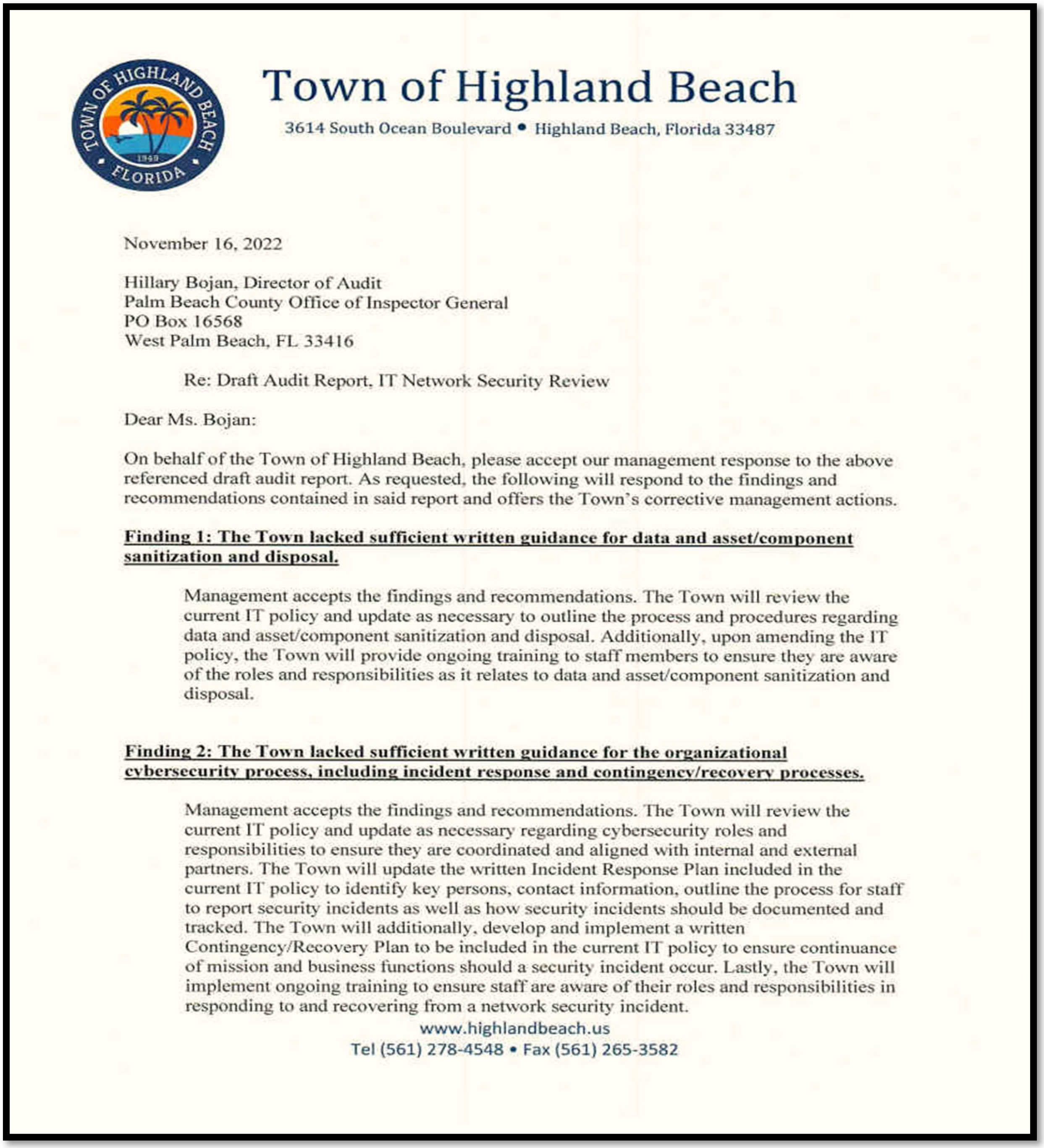
The Inspector General's audit staff would like to extend our appreciation to the Town of Highland Beach's staff for their assistance and support in the completion of this review.

This report is available on the OIG website at: http://www.pbcgov.com/OIG. Please address inquiries regarding this report to the Director of Audit by email at inspector@pbcgov.org or by telephone at (561) 233-2350.

ATTACHMENT

Attachment 1 – Town of Highland Beach's Management Response

ATTACHMENT 1 – TOWN OF HIGHLAND BEACH'S MANAGEMENT RESPONSE



Town of Highland Beach

3614 South Ocean Boulevard • Highland Beach, Florida 33487

November 16, 2022

Hillary Bojan, Director of Audit
Palm Beach County Office of Inspector General
PO Box 16568
West Palm Beach, FL 33416

Re: Draft Audit Report, IT Network Security Review

Dear Ms. Bojan:

On behalf of the Town of Highland Beach, please accept our management response to the above referenced draft audit report. As requested, the following will respond to the findings and recommendations contained in said report and offers the Town's corrective management actions.

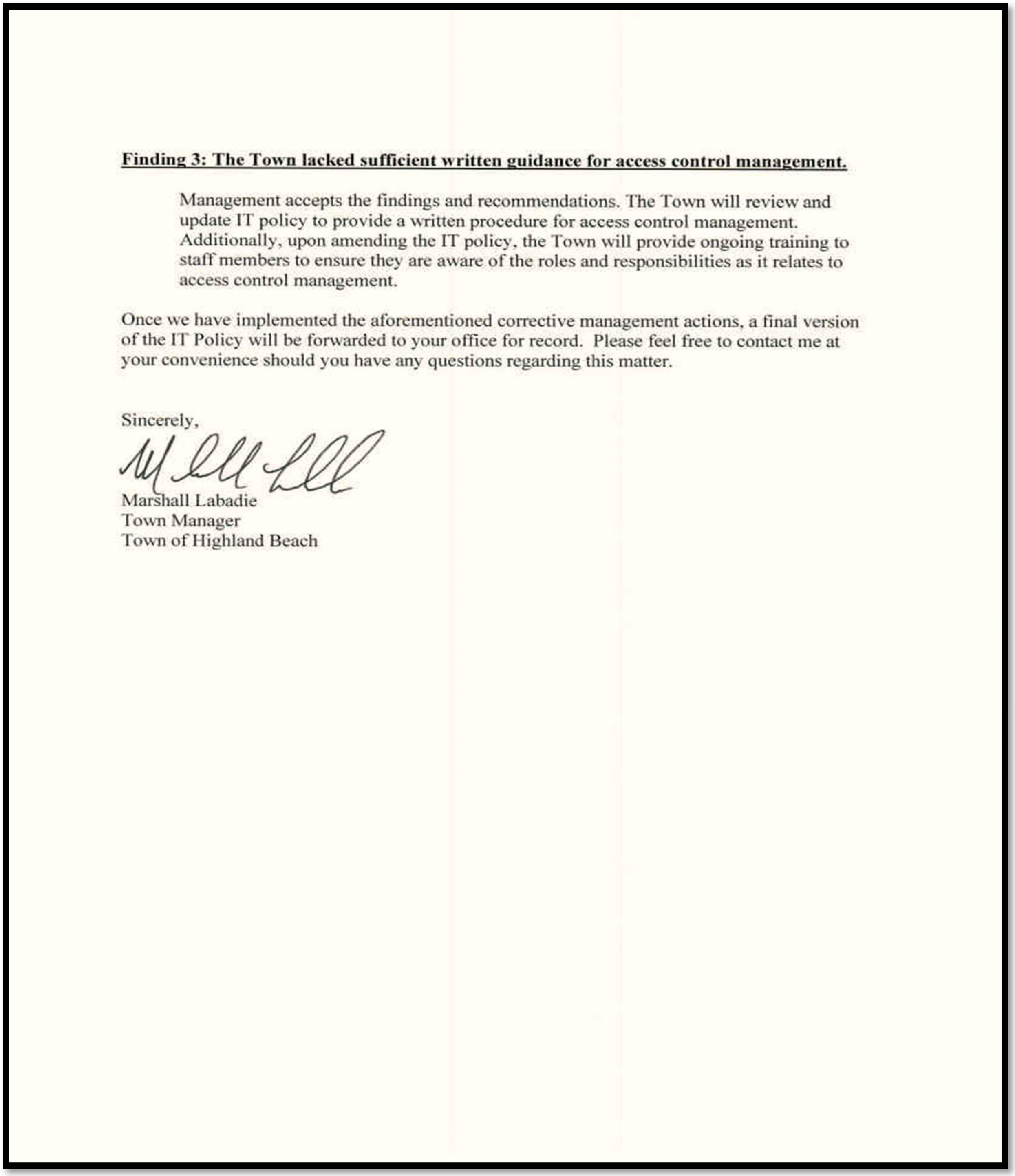
Finding 1: The Town lacked sufficient written guidance for data and asset/component sanitization and disposal.

Management accepts the findings and recommendations. The Town will review the current IT policy and update as necessary to outline the process and procedures regarding data and asset/component sanitization and disposal. Additionally, upon amending the IT policy, the Town will provide ongoing training to staff members to ensure they are aware of the roles and responsibilities as it relates to data and asset/component sanitization and disposal.

Finding 2: The Town lacked sufficient written guidance for the organizational cybersecurity process, including incident response and contingency/recovery processes.

Management accepts the findings and recommendations. The Town will review the current IT policy and update as necessary regarding cybersecurity roles and responsibilities to ensure they are coordinated and aligned with internal and external partners. The Town will update the written Incident Response Plan included in the current IT policy to identify key persons, contact information, outline the process for staff to report security incidents as well as how security incidents should be documented and tracked. The Town will additionally, develop and implement a written Contingency/Recovery Plan to be included in the current IT policy to ensure continuance of mission and business functions should a security incident occur. Lastly, the Town will implement ongoing training to ensure staff are aware of their roles and responsibilities in responding to and recovering from a network security incident.

www.highlandbeach.us
Tel (561) 278-4548 • Fax (561) 265-3582



Finding 3: The Town lacked sufficient written guidance for access control management.

> Management accepts the findings and recommendations. The Town will review and update IT policy to provide a written procedure for access control management. Additionally, upon amending the IT policy, the Town will provide ongoing training to staff members to ensure they are aware of the roles and responsibilities as it relates to access control management.

Once we have implemented the aforementioned corrective management actions, a final version of the IT Policy will be forwarded to your office for record. Please feel free to contact me at your convenience should you have any questions regarding this matter.

Sincerely,

Marshall Labadie
Town Manager
Town of Highland Beach