OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

John A. Carey
Inspector General

Inspector General
Accredited

*"Enhancing Public Trust in Government"*

# Audit Report

# 2023-A-0004

# City of Atlantis - IT Network Security Review

# March 23, 2023

OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

AUDIT REPORT
2023-A-0004

DATE ISSUED: MARCH 23, 2023

John A. Carey
Inspector General

Inspector General
Accredited

*"Enhancing Public Trust in Government"*

# CITY OF ATLANTIS - IT NETWORK SECURITY REVIEW

## SUMMARY

### WHAT WE DID

We conducted an Information Technology (IT) Network Security review of the City of Atlantis (City).[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 fiscal year (FY) 2022 through January 24, 2023.[2]

### WHAT WE FOUND

We found that the City 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, we found weaknesses with respect to inventory and control of enterprise assets and organizational cybersecurity training. The City also lacked sufficient written guidance for: (a) access control management; (b) data asset/component sanitization and disposal, and (c) organizational cybersecurity processes, including incident response and contingency/ recovery processes.

### WHAT WE RECOMMEND

Our report contains five (5) findings and 13 recommendations. Implementation of the recommendations will assist the City in strengthening internal controls over IT Network Security.

The City of Atlantis did not provide us with a written response to the report findings and recommendations.

---

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

[2] Due to delays caused by the City, the initial review scope that included IT network security records and activities related to IT network components, such as devices, systems, and data, in place during FY 2022 was expanded through January 24, 2023, the date of our final interview.

## BACKGROUND

The City of Atlantis (City) was incorporated in 1959 by the Laws of Florida, Chapter 59-1055. City Ordinance No. 240, adopted January 20, 1993, substantially amended the original City Charter. Atlantis was originally an 834-acre development formerly known as Mulberry Farms and owned by former State Senator Philip D. Lewis, to raise Brahman cattle. The development was purchased in 1958 to develop a country club community with an 18-hole golf course. Based on 2020 Census Data, the City's 2020 population was approximately 2,142.[3]

The government of the City is vested in the City Council which is composed of five (5) members elected to staggered two (2) year terms. The members of the City Council appoint one (1) member a Mayor and another a Vice-Mayor of the City, each for a one (1) year term. The Mayor is the chief executive officer of the City, under the overall supervision of the City Council, and with the aid of the City Manager. The City Council appoints the City Manager, who is the administrative head of the City.

The OIG FY 2022 Annual Audit Plan included IT Network Security Reviews. The City of Atlantis 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 City's IT Network Security risk. Additionally, the City is small in terms of size and budget compared to many municipalities in Palm Beach County and operates a Police department; both factors further increase IT Network Security risk.[4]

### Review Delays

On May 11, 2022, the OIG delivered its IT Network Security Review engagement letter to the City detailing our objectives, scope, and methodology (see page 9 of this report). As a follow-up to the engagement letter, on May 16, 23, 25, 31, and June 8, 2022, we provided the City with an array of proposed entrance conference dates and times.

On June 14, 2022, the City Manager emailed the Inspector General to inform the OIG that since 2019, the City completed an internal audit, the Florida Department of Law Enforcement (FDLE) completed an IT audit, the City's liability carrier completed an audit, and the City's new Enterprise Resource Planning (ERP) system provider completed an audit. (The City Manager later acknowledged during sworn testimony that these reviews, with the exception of the FDLE audit, were not formal audits.[5]) The City Manager requested that in light of the multiple audits completed since 2019, OIG help him "better

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

[4] The PBC OIG Inspector General informed the City's Council that the City's increased risk was the reason for its selection for an IT Network Security Review at its June 15, 2022 Council meeting.

[5] Formal audits are independent and conducted using professional auditing standards.

understand" the IG's goals for its review. The City Manager also asked to schedule the entrance conference sometime after the City's July 20, 2022, Council Meeting.

On June 15, 2022, at the City's regularly scheduled council meeting, the Inspector General provided the City Council with background information explaining why the OIG was conducting network security reviews throughout Palm Beach County. The Inspector General informed the Council that he would accommodate the City's request to delay the review until after July 20, 2022, and that his presentation would be considered our entrance conference.

> On August 1, 2022, the OIG provided the City proposed dates and times for the on-site interview/walk-through and our initial documentation request list. On August 10, 2022, the OIG followed up on this request. The City Manager responded, "We will check with our IT consultants for availability."

During the period between August 31 and September 20, 2022, the OIG followed up with the City on four (4) separate occasions to schedule a time for the interview/walk-through meeting.

On October 5, 2022, the Inspector General reminded the City Manager via email that, at his request, the office agreed to delay the network security review until after July 20, 2022. The Inspector General stated that the review had been delayed for almost five (5) months and the office needed to schedule its on-site interviews. The City Manager did not acknowledge or respond to this request.

On October 17, 2022, the OIG, forwarded the October 5, 2022 correspondence to the City Clerk, requesting she acknowledge receipt. The City Clerk did not respond.

On October 19, 2022, the Inspector General sent the October 5 and October 17, 2022, communications to the City Council requesting that the City contact the OIG so that it could begin the network security review process.
On October 21, 2022, the City Manager requested an in-person meeting with the Inspector General sometime during the following week.

On November 14, 2022, the parties met at the OIG office in West Palm Beach. At the conclusion of this meeting, the Inspector General and the City Manager agreed to an on-site interview/walk-through on November 30, 2022.

On November 29, 2022, the City Manager communicated the following to the Inspector General:

> Following direction from the City Council at our most recent public meeting, I will not be able to meet with the OIG

regarding an audit of the City's cybersecurity polices, practices, and procedures.

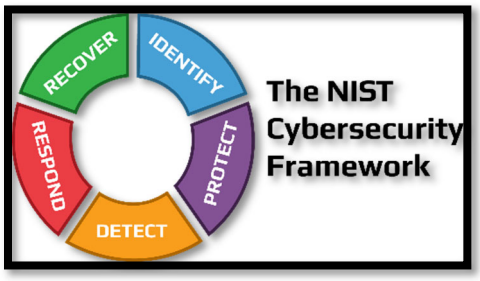
On December 15, 2022, pursuant to the authority of Palm Beach County Code Article XII, Inspector General, Sec. 2-423(3), the OIG issued subpoenas to: (1) City Clerk, Records Custodian, City of Atlantis, for records related to conducting the IT Network Security Review; (2) City Manager, City of Atlantis, for testimony related to the IT Network Security Review; and, (3) IT Consultant, for the City of Atlantis, for testimony related to the IT Network Security Review.

The OIG received records from the City on January 10, 2023; sworn testimony from the City Manager on January 17, 2023; and testimony from the City's IT Consultant on January 24, 2023.

## OIG IT NETWORK SECURITY REVIEW CHECKLIST

### NIST Framework

The National Institute of Standards and Technology (NIST)[6] created a cybersecurity risk framework for use by critical infrastructure owners and operators. The NIST Framework Core consists of five interrelated functions—Identify, Protect, Detect, Respond, and Recover.




- **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.
- **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[7] establishes controls for systems and organizations that process, store, or transmit information. The publication was designed

[6] As part of the U.S. Department of Commerce, NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. Additionally, the State of Florida Cybersecurity Standards are modeled after the NIST Framework and the Federal Information Security Management Act of 2002. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

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

to help organizations identify the controls necessary to manage security and privacy risk and is intended to be used by a diverse audience.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse audience, including:

- 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 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
- Personally Identifiable Information Processing and Transparency
- Awareness and Training
- Contingency Planning
- Incident Response
- Risk Assessment

**CIS Critical Security Controls**

The Center for Internet Security (CIS)[8] 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

[8] 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

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. IG 1 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

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 for Improving Critical Infrastructure Cybersecurity Version 1.1 (Framework) 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 Center

for Internet Security (CIS) Critical Security Controls (Version 8) IG 1,[9] 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:

1. Physical Devices (Hardware) Account Management (User and Administrative)
2. Organizational Cybersecurity Policy
3. Access Control Management
4. Disposition of Data
5. Malware Defenses
6. Email and Web Browser Protections
7. Network Security Awareness Program and Training
8. Incident Management Response Plan
9. Contingency/Recovery Planning

We shared this checklist with the State of Florida's Chief Inspector General and Chief Information Security Officer (CISO).

## OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objectives of the review were to determine whether the City 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 fiscal year (FY) 2022 through January 24, 2023 through January 24, 2023.

The City imposed significant constraints on our review approach by denying on-site access to City IT network resources, records, and individuals. We completed this review based on records provided pursuant to a subpoena and sworn testimony from the City Manager and testimony from the City's IT Consultant. As a result, we were not able to observe how certain reports were generated by the City (*e.g., employee master file and user accounts in Active Directory)*, or observe IT network resources and settings such as password criteria, screensaver activation, and the time duration before being locked out of an application.

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;

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

- Interviewing appropriate personnel; and,
- Reviewing records, logs, and reports.

This review was conducted in accordance with 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.

## FINDINGS AND RECOMMENDATIONS

### Finding (1): The City lacked an accurate enterprise asset inventory list of network system components.

The NIST Framework describes asset management as identifying and managing data, personnel, devices, systems, and facilities that enable an organization to achieve its business purposes. Physical devices, systems, software, and applications within the organization should be inventoried. The NIST Security and Privacy Controls for asset management includes developing an accurate system component inventory that is periodically updated. Additionally, the CIS Critical Security Controls IG 1 includes actively managing (inventory, track, and correct) all enterprise assets connected to the network to accurately know the totality of the assets that need to be monitored and protected within the enterprise.

Inventory of Enterprise Asset controls include:

- Establish and maintain a detailed and accurate asset inventory list (machine name, static network address, hardware address, enterprise asset owner and, department) of all network components;
- Update the inventory list when components are installed or removed; and,
- Address unauthorized assets, e.g. hardware, software and firmware components.

The City provided us with an enterprise asset inventory list pursuant to our records subpoena; however, the list was not fully populated, lacked certain key controls, and may have been incomplete.

We identified the following Inventory of Enterprise Asset control exceptions:

- The asset inventory list did not always include the machine/device name or other unique identifier;
- The asset inventory list did not include the static network address or hardware address; and,
- Although the City Manager and the City's IT consultant reviewed and affirmed the accuracy of the City's asset inventory list, there was a discrepancy between the number of components identified on the list and statements made by the IT consultant. Specifically, the asset inventory list identifies 24 components, while the IT consultant said he knew the list was accurate because the City had less than

40 users and about 35 total pieces of equipment. The OIG attempted to clarify this discrepancy with the City and its IT consultant; however, they have been unresponsive.

During sworn testimony on January 17, 2023, the City Manager stated that the inventory list was prepared the prior week and is updated as needed. The IT Consultant confirmed that the City updates the list after work is performed. Potentially, the City's inventory list was not compared to the components and devices connected to the network to ensure that all components and devices were included in the inventory list and no unauthorized components or devices were connected to the network.

An inaccurate or incomplete enterprise asset inventory list increases risk associated with unauthorized components accessing the network and loss of control over protected or sensitive data.

### Recommendations:

**(1) The City update its enterprise asset inventory list to ensure it includes all network components or devices and provides, at a minimum, the:**

- **a. Machine name;**
- **b. Static network address;**
- **c. Hardware address;**
- **d. Enterprise asset owner; and,**
- **e. Department.**

**(2) The City update its inventory list when components are installed or removed.**

**(3) The City routinely compare its enterprise asset inventory list to the network components and devices and address unauthorized assets.**

### Management Response:

**The City of Atlantis did not respond to the report findings and recommendations.**

### Finding (2): The City lacked sufficient organizational cybersecurity training, to include social engineering attacks, such as phishing emails and tailgating.

The NIST Framework describes information protection processes and procedures as security policies, processes, and procedures that are maintained and used to manage protection of information systems and assets. The NIST Security and Privacy Controls for training and awareness include providing security and privacy literacy training to system users to include incident response training and information protection processes and procedures to include having system and information integrity policies and procedures for spam protection at network entry and exit points that detect and act on unsolicited messages. Additionally, the CIS Critical Security Controls IG 1 includes security

awareness and skills training controls that influence staff behavior by enhancing their security consciousness and detection skills to reduce cybersecurity risks.

Information protection/security awareness and skills training controls include:

- Establish and maintain a security and privacy awareness program;
- Train staff to recognize social engineering attacks, such as phishing, pre-texting, and tailgating;
- Train staff on authentication best practices (e.g. MFA, password composition, and credential management);
- Train staff on data handling best practices, including how to identify and properly store, transfer, archive, and destroy sensitive data, clear screen and desk best practices, and storing data and assets securely;
- Train staff on causes of unintentional data exposure (e.g. mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences);
- Train staff on recognizing and reporting security incidents;
- Train staff on how to identify and report if their enterprise assets are missing security updates;
- Train staff on the dangers of connecting to and transmitting enterprise data over insecure networks; and,
- Update security and privacy training and awareness content and incorporate lessons learned into training and awareness techniques.

We found that the City has processes with controls to assist with information protection; however, the City has no cybersecurity awareness and training program and staff has not been provided with any security awareness and skills training.

The City Manager stated that in the past the City did not have the capability to provide security awareness and skills training to its staff. However, after replacing all of the City's hardware and software, he directed the City's IT consultant to implement phishing training.[10]

Additionally, the City Manager stated that although the City has discussed providing security awareness and skills training, implementation has been delayed because they are waiting for the State of Florida to issue its mandated cybersecurity training[11] requirements.

A lack of information protection/security awareness and skills training increases the risk associated with ransomware attacks and loss of control over protected or sensitive data. The State of Florida mandated cybersecurity training for local governments has not yet

[10] The IT consultant confirmed to the OIG that security awareness and skills training for phishing attacks will be implemented during the first quarter of 2023.

[11] Section 282.3185(3) states that Florida Digital Service will develop a basic cybersecurity training curriculum for local government employees, and all employees with access to the local government's network must complete the training within 30 days after commencing employment and annually thereafter. Florida Digital Service is an organization created by the State of Florida in 2020 to leverage data and deploy technology to better serve Floridians.

been issued. Nevertheless, the threat to local governments posed by network security incidents, including ransomware attacks, currently exists. We have identified 12 network security incidents affecting local government entities in and around Palm Beach County within the last four years, four of which involved municipalities within Palm Beach County.

On December 22, 2023, the Inspector General met with the State of Florida CISO to discuss our IT Security audits and reviews. He concurred that cities should not wait on future state guidance to conduct training or delay our audits and reviews. Municipalities can best protect themselves and their assets by instituting a security awareness and skills training program to address current threats instead of waiting for future guidance from the State of Florida on a date yet to be determined.

**Corrective Action:**
On January 10, 2023, the City Clerk provided our office with the City's Technology Resource Policy that includes a section on Information Security Education and Training. However, the effective date of the Technology Resource Policy is not clear; OIG Finding #3 discusses this issue in detail.

We reviewed the City's Technology Resource Policy implemented during our review and found that it requires all employees to complete annual training on information security awareness and concepts; practice security awareness; to immediately report incidents involving any City accounts, concerns or suspicious activities; and to note and report observed or suspected security weaknesses to systems and services. However, the policy does not include recognizing social engineering attacks, authentication best practices, data handling best practices, causes of unintentional data exposure, recognizing security incidents, identifying if enterprise assets are missing security updates, and dangers of connecting to and transmitting enterprise data over insecure networks.

## Recommendations:

**(4) The City should establish and maintain an Information Protection/Security Awareness and Skills Training program that provides guidance, at a minimum, including:**

- **a. Recognizing social engineering attacks;**
- **b. Authentication best practices;**
- **c. Data handling best practices;**
- **d. Causes of unintentional data exposure;**
- **e. Recognizing and reporting security incidents;**
- **f. Identifying and reporting if their enterprise assets are missing security updates; and,**
- **g. Dangers of connecting to and transmitting enterprise data over insecure networks.**

**(5) Provide staff with ongoing Information Protection/Security Awareness and Skills Training.**

## Management Response:

**The City of Atlantis did not respond to the report findings and recommendations.**

## Finding (3): The City 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 assessed risk of unauthorized access to authorized devices and transactions. The NIST Security and Privacy Controls for access control management processes includes having account management, access enforcement, separation of duties, least privilege,[12] access control for mobile devices, and identification and authentication processes and procedures. The CIS Critical Security Controls IG 1 includes processes and tools to assign and manage authorization to credentials as well as create, assign, manage, and revoke access credentials and privileges for user, administrative, and service accounts; and, establishing and maintaining secure configuration of enterprise assets (end-user devices; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

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; and,
- Enabling device lock features (screensavers, blank screens, etc.) preventing network access when users are away from their workspace.

We found that the City 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, employing the principal of least privilege, and maintaining secure configuration of enterprise assets and software to include requiring

[12] 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.

unique user IDs and passwords, automatic logouts after periods of inactivity, screensavers, and multifactor authentication. However, there were no written IT policies or procedures in place at the time of our review. According to the City Manager, the City did not have any IT network security polices prior to October 2022.

**Corrective Action:**

On January 10, 2023, the City Clerk provided our office with the City's Technology Resource Policy, Computer Usage Policy, and Data Protection & Recovery Policy pursuant to a records subpoena. The Computer Usage Policy was documented with an effective date of December 16, 2022. The effective dates of the Technology Resource and Data Protection and Recovery policies were not included on the documents provided. The City Manager, during his sworn testimony on January 17, 2023, explained the policies, without effective dates were implemented in October 2022.

Following the City Manager's sworn testimony, the OIG listened to various City Council Meetings to confirm the policy implementation date. At the October 19, 2022 meeting, the City Manager distributed a draft copy of its "Information Security" and "Computer Use" policies. At the November 16, 2022 meeting, the City Manager again distributed the "Information Security" policy and stated that this copy is the same document that was provided during the October 19, 2022 meeting. Moreover, he stated additional copies of the draft polices were provided to the City Attorney, for a legal sufficiency review, to the City's IT Consultant for its review, and to the City Council for its review. The City Manager requested that the City Council provide him with any comments prior to, or during, the next City Council Meeting. The City Manager stated that any proposed changes to the draft policies, either by the City Council or the City's IT Consultant, would be taken into consideration before finalization. Once finalized, the policies would be given an effective date. We did not identify any additional public comment concerning the City's information technology polices after the November 16, 2022 meeting.

We found that the Technology Resources Policy the City Clerk provided to the OIG in January 2023 is more robust than the "draft" Information Security Policy provided to the City Council in October and November 2022. It is unclear when it was revised, renamed, or the effective date thereof. The OIG requested clarification from the City; however, we did not receive a response. Regardless of whether the City's Technology Resource Policy was in effect in October 2022, November 2022, or January 2023, we assess our engagement notification in May 2022 may have had the positive effect of encouraging the City to create this policy.

We reviewed the City's Technology Resource Policy provided during our review and found that it provides for the removal of access rights upon changes in employment role or transfer between departments shall require the Technology Resources Administrator approval to ensure granted permissions and authorizations are appropriate for the new role. Additionally, the policy has provisions for: (a) protecting confidential data; (b) access rights based on the principle of least privilege; (c) restricting administrator privileges; (d) process for escalating or de-escalating rights; (e) data classification; (f) default access privileges; (g) notification process in case of a data security breach; (h) remote access

methods, with security measures; (i) password construction and protection; and, (j) screensaver usage.

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 unauthorized users may be able to gain access to the system due to weak configuration settings and users have access to critical or sensitive data and systems that is not necessary to perform their roles and responsibilities within the organization.

### Recommendations:

**(6) The City develop and implement a written access control management policy and procedure that provides guidance, at a minimum, 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;**
- **g. Establishing unique identification and authentication requirements (usernames, passwords, biometrics, etc.) for user accounts accessing the network; and,**
- **h. Enabling device lock features (screensavers, blank screens, etc.) preventing network access when users are away from their workspace.**

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

### Management Response:

**The City of Atlantis did not respond to the report findings and recommendations.**

### Finding (4): The City 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 IG 1 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 City had processes with controls to assist with data and asset/component sanitization and disposal; however, there were no written IT policies or procedures in place at the time of our review. According to the City Manager, the City did not have any IT network security polices prior to October 2022.

**Corrective Action:**

On January 10, 2023, the City Clerk provided our office with the City's Technology Resource Policy that includes a section on Disposal of Media. However, the effective date of the Technology Resource Policy is not clear; OIG Finding #3 discusses this issue in detail.

We reviewed the City's Technology Resource Policy provided during our review and found that it provides guidance for data retention limits and disposal requirements and ensures the disposal process and method is commensurate with the data sensitivity; however, the policy does not include 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; remote purging or wiping of data on lost or stolen organizational assets; testing of sanitation equipment and procedures; verification that the sanitization of the asset was effective prior to disposal.

## Recommendations:

**(8) The City develop and implement a written Data Sanitization and Asset/Inventory Disposal policy and procedure that provides guidance regarding:**

- **a. Establishing and maintaining a data management process that addresses data retention limits and disposal requirements and ensures 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 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;**
- **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.**

**(9) The City ensure staff are aware of their roles and responsibilities related to data and asset/component sanitization and disposal.**

## Management Response:

**The City of Atlantis did not respond to the report findings and recommendations.**

## Finding (5): The City 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 IG 1 includes establishing an Incident Response Management process 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; and, 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 for staff to report security incidents;
- Testing to determine the effectiveness of the plan to identify weaknesses or deficiencies; 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;
- Addressing eventual, full system restoration without deterioration of the controls originally planned;
- Testing to determine the effectiveness, and readiness, of the plan to identify potential weaknesses; and,
- Safeguarding and testing of backup information to ensure it can be reliably retrieved and restored for essential mission and business functions.

We found that the City had processes with controls to assist with continuity of operations should it be exposed to a cybersecurity incident; however, there were no written IT policies or procedures in place at the time of our review. According to the City Manager, the City did not have any IT network security polices prior to October 2022. Additionally, during the City Manager's sworn testimony and the IT Consultant's testimony, each provided different system restoration priorities.

**Corrective Action:**

On January 10, 2023, the City Clerk provided our office with the City's Technology Resource Policy, Computer Usage Policy, and Data Protection & Recovery Policy that include guidance related to the City's incident response and contingency/recovery activities. However, the effective date of the Technology Resource and Data Protection & Recovery policies is not clear; OIG Finding #3 discusses this issue in detail.

We reviewed the Technology Resource Policy and Computer Usage Policy provided to our office and found that it designated responsibilities for and established processes to manage and monitor cybersecurity risks, including an Incident Response plan; however, the plan does not identify how the City plans to communicate information to leadership and employees, and it has not been fully tested.

Additionally, we reviewed the Data Protection & Recovery Policy provided to our office. The policy did not include a sufficient Contingency/Recovery plan because it 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); address eventual, full system restoration without the deterioration of the controls originally planned and implemented; and, the safeguarding and testing of backup information to ensure it can be reliably retrieved and restored for essential mission and business functions.

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. Conflicting restoration priorities could result in delays restoring critical business systems.

## Recommendations:

**(10) The City implement an 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.**

**(11) The City develop and implement written Incident Response Plan policies and procedures to ensure continuity of operations that provide guidance, at a minimum, 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;**
- **d. Testing to determine the effectiveness of the plan to identify weaknesses or deficiencies; and,**
- **e. Tracking and documenting security incidents.**

**(12) The City develop and implement written Contingency/Recovery Plan policies and procedures to ensure continuance of mission and business functions that provide guidance, at a minimum, 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;**
e. **Addressing eventual, full system restoration without deterioration of the controls originally planned;**
f. **Testing to determine the effectiveness, and readiness, of the plan to identify potential weaknesses; and,**
g. **Safeguarding and testing of backup information to ensure it can be reliably retrieved and restored for essential mission and business functions.**

**(13) The City 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:

**The City of Atlantis did not respond to the report findings and recommendations.**

*This report is available on the OIG website at: https://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.*