



Performance Audit

Citywide Review of Department and Authority Policies Concerning the Management of Personally Identifiable Information

Report by the
Office of City Controller

**MICHAEL E. LAMB
CITY CONTROLLER**

Douglas W. Anderson, Deputy Controller

Gloria Novak, Performance Audit Manager

Bette Ann Puharic, Assistant Performance Audit Manager

Mark Ptak, Research Assistant

Ryan Herbinko, Solicitor

November 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
INTRODUCTION	1
OVERVIEW	1
OBJECTIVES	3
SCOPE	3
METHODOLOGY	3

FINDINGS & RECOMMENDATIONS

Citywide PII Policies	5
Collecting and Retaining PII.....	5
Personnel and Civil Service Commission Policies	6
PII Recommended Best Practices Model.....	6
Record Retention Policies	7
City Ordinance No. 19 (2012)	8
Document Shredding	8
Open Records and Open Data (Right to Know Law)	9
Electronic PII Security	11
Employee PII Awareness and Training	13

FIGURES

Figure 1: Burgh’s Eye View Screen Shot.....	10
Figure 2: Phishing Scam Example	13
Figure 3: City Employee Email Scam	14

November 15, 2017

To the Honorables: Mayor William Peduto and
Members of Pittsburgh City Council:

The Office of the City Controller is pleased to present this audit of **Citywide Review of Department and Authority Policies Concerning the Management of Personally Identifiable Information**, conducted pursuant to the Controller's powers under Section 404(b) of the Pittsburgh Home Rule Charter.

EXECUTIVE SUMMARY

Personally Identifiable Information (PII) covers a broad range of personal data that could be used to identify a specific individual. While all city departments and authorities handle PII in some manner, some interact with this information more than others, particularly the Department of Innovation and Performance and the Department of Personnel and Civil Service Commission.

This audit examines how secure the policies and procedures of departments and authorities are in protecting the PII they come in contact with. We met with various representatives to assess the security of their conduct as it relates to PII, identify areas for improvement, and outline a comprehensive, citywide strategy to safeguard PII data and documents.

While there are various federal and state statutes governing payroll, financial information, and data collected for federal assistance programs, there is no citywide policy covering the safe collection storage, transmission, or disposal of PII data. Procedures are generally set by leadership and tradition, but the city would benefit from uniform, standardized enforcement on this particular topic.

Likewise, as a city of the second class, Pittsburgh is exempt from the state's Municipal Records Act, and does not have record retention schedules in place to uniformly destroy documents kept past their legal usefulness. Efforts have been made in recent years to establish schedules in each department through the Commission on City Archives, but a lack of progress led that effort to be

undertaken by the city archivist. Such schedules would allow documents containing sensitive PII to be securely destroyed, particularly in personnel.

The Department of Innovation and Performance has taken a proactive role in combatting external threats from hackers and phishing scams that seek to steal personal information. The auditors found that more could be done to prevent internal compromises of PII by using endpoint security software, collaborating with personnel to immediately terminate user accounts after an employee leaves the city payroll, developing a data breach response policy, and considering the purchase of cyber security insurance.

The city would also benefit from greater employee awareness of what PII is, the threats that could compromise its security, and the resources at their disposal to avoid them. The auditors found that this could be achieved through ongoing PII cybersecurity training and a formal encryption procedure when transmitting sensitive information through email.

Our findings and recommendations are discussed further beginning on page five. We believe our recommendations will give guidance to developing citywide PII policies and procedures.

We would like to thank all city and authorities' representatives we met with for their cooperation and assistance during our audit.

Sincerely,

Michael E. Lamb
City Controller

INTRODUCTION

This performance audit regarding city departments and authorities' management of personally identifiable information was directed by City Council and conducted pursuant to section 404(c) of the Pittsburgh Home Rule Charter. The City Council resolution authorizes the City Controller "to perform an audit of Department policies that pertain to the acquisition, retention, and destruction of personally identifiable information."

This is the first performance audit conducted on personally identifiable information and assesses current policies and procedures in place throughout city departments and authorities.

OVERVIEW

The most commonly cited definition of personally identifiable information (PII) is found in the White House Office of Management and Budget's memorandum M-17-12 (January 3, 2017):

(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

This definition also notes that:

Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available - in any medium or from any source - that would make it possible to identify an individual.

For example, a name alone may not be considered PII, but could result in identity theft if paired with a partial social security number or date of birth. Also, discrimination could occur if paired with race, religion, sexual orientation or medical information, etc.

In addition, the digitization of paper records presents new challenges in protecting personal information. The recent surge of data breaches and identity theft in the private and public sectors have demonstrated that while electronic records can reduce costs and improve the efficiency of city services, they also leave government entities vulnerable to the breach of personal information on an unprecedented scale.

For instance, in 2015 the federal Office of Personnel Management (OPM) became the target of one of the largest personal data breaches in US history, affecting the PII of over 20 million people, including social security numbers, names, dates and places of birth, and addresses.

As recently as September 2017, that breach was eclipsed by the hacking of credit agency Equifax, with as many as 143 million U.S. consumers' personally identifiable information stolen and made vulnerable to identity theft. Without constant maintenance of their information systems' security and infrastructure, local governments may be vulnerable to similar attacks. A 2014 report by the Federal Trade Commission (FTC) shows Pennsylvania ranking 16th in states reporting the most identity theft complaints per capita, highlighting the seriousness of the threat.

While hackings and phishing scams are some of the more widely publicized examples of PII being compromised, violations can also occur internally, whether intentional or unintentional. This includes an employee accessing PII when they are not authorized to do so, PII records that leave an office or are transferred onto a personal device, posting or sending PII on social media, or intentional theft of personal information by an employee.

Any comprehensive strategy to prevent those efforts should:

- identify what personally identifiable information is
- take a full, detailed inventory of all PII held
- limit the amount of PII collected and/or duplicated to the minimum necessary for a department to accomplish its goals
- have clear and secure policies in the collection, storage, transmission, and disposal of PII regularly educate employees on how to securely handle PII and avoid external threats
- closely monitor potential external and internal threats to personal data stored electronically
- develop data breach response policies that effectively mitigate damages and prevent future incidents.

OBJECTIVES

1. Examine the policies that are currently in place to safeguard personal information and identify deficiencies that could lead to its loss, theft, or unauthorized access
2. Research best practices for the collection, storage, transmission, and disposal of personally identifiable information
3. Make recommendations for improvements

SCOPE

The scope of this performance audit identifies existing policies and practices for securing personally identifiable information in all city departments and authorities for 2017.

METHODOLOGY

The audit staff met with representatives of various city departments and authorities to discuss PII policies and procedures. These included: Personnel and Civil Service Commission (PCSC); Innovation and Performance (I&P); Law; Permits, Licenses, and Inspections (PLI); Commission on Human Relations; Public Safety; Finance; Animal Care and Control; Office of Management and Budget (OMB); Office of the City Clerk; Parking Authority; Allegheny Regional Asset District (ARAD); Sports and Exhibition Authority (SEA); and the Office of the City Controller. They also met with members of the Mayor's executive team as well as the City Archivist. The auditors attempted to meet with representatives from the Pittsburgh Water and Sewer Authority (PWSA) and the Urban Redevelopment Authority (URA), but did not receive a response. The Housing Authority declined a meeting.

Existing policies in the public sector concerning PII were examined as benchmarks for recommendations. At the federal level, this included the White House Office of Management and Budget, the General Service Administration, the Department of Homeland Security, and the Department of Labor. At the state level, this included the Municipal Records Manual issued by the Pennsylvania Historical and Museum Commission for the Bureau of Archives and History. The experience of various municipalities in handling PII was also studied.

Examples of any written or existing policies were requested and provided where available. Auditors reviewed the Police Bureau's media and privacy policy, Pennsylvania's Right to Know Law and Breach of Personal Information Act, the 2012 City Council ordinance establishing the Commission on city Archives, Personnel's draft record retention schedules, the Sports and Exhibition Authority's cyber insurance policy, the Parking Authority's data classification and vendor information security policies, the PA Bureau of Archives and History's Municipal Records Manual, and the White House Office of Management and Budget's M-07-16

directive. Auditors also reviewed comparable state and local legislation, including Massachusetts' 2007 PII law and a 2016 PII audit by the city of Denver's auditor.

Auditors held biweekly meetings with the city's departments of Personnel and Civil Service and Innovation and Performance as a result of this audit to help develop PII security and retention policies.

FINDINGS & RECOMMENDATIONS

Citywide PII Policies

PII is collected in some form by every department and authority and applies to both employees and residents of the city. The auditors found that city departments and authorities generally understood the importance of having secure PII policies in place, but enforcement and communication is inconsistent.

Some departments and authorities are obligated to follow established federal or state policies. For example, states that receive federal funding must abide by strict federal requirements in handling and sharing PII when distributing funds to municipal housing authorities such as Pittsburgh's Housing Authority. PII can only be transferred through the secure state portal; hard copies can only be printed by authorized users and must be kept in a vault when not in use. Fax machines must be kept in a locked location only accessible to authorized employees, and a regular retention schedule is in place to securely destroy records after seven years.

Finding: There is no citywide policy defining PII. This can leave the city vulnerable between administrations or leadership vacancies.

Finding: There is no comprehensive citywide policy regarding the safe collection, storage, transmission, or disposal of PII.

The nonexistence of a policy can result in the city being at risk for having PII information compromised. This also could cause increased litigation costs and damages paid out to those affected, as well as harm to the city's reputation.

RECOMMENDATION NO. 1:

City Council should establish a uniform definition of PII that applies to all departments, authorities, contractors, city employees and residents. The White House OMB's broad, context-inclusive definition is recommended as a model as explained in the overview.

Collecting and Retaining PII

The auditors found that two departments come into contact with the highest volume of PII: Personnel & Civil Service Commission (PCSC), because it manages sensitive employee information, and Innovation & Performance (I&P), because it manages the city network and protects potentially sensitive information located on its servers.

Personnel and Civil Service Commission Policies

Due to the sheer volume of PII documents handled by PCSC on a daily basis, it is unrealistic to expect its employees to keep that information locked when unsupervised. To mitigate the risk of unauthorized dissemination of information, all employees are considered authorized to handle the personal information the department takes in, and the entire office is kept locked at all times, only accessible if an employee lets a non-employee in. One exception is the cleaning staff, which has access to the office to change waste bins at night.

Finding: PCSC safeguards the high volume of personal information it handles by generally keeping the entire office a closed and secure area.

RECOMMENDATION NO. 2:

PCSC should keep the office a closed and secure area after work hours when authorized employees are gone for the day by leaving waste bins outside so cleaning staff does not have access to the area.

Finding: Currently, PCSC's records and files are paper documents. Paper documents become cumbersome and bulky.

For example, the City Controller's Office's uses OnBase software, which enables employees to scan documents into a searchable database managed by I&P, significantly cutting down on storage and waste.

RECOMMENDATION NO. 3:

PCSC should strongly consider investing in an electronic scanning system to store documentation. An electronic filing system would reduce paper waste and costs, improve efficiency, and reduce the risk of losing personal information.

RECOMMENDATION NO. 4:

City Council, in collaboration with the city archivist, PCSC and I&P should develop written policies governing the collection, storage and disposal of PII.

PII Recommended Best Practices Model

The auditors researched best practices covering PII. Based on the existing body of best practices, the auditors recommend that those written policies contain at minimum the following:

- a full inventory of PII intake points and a flow chart of where that information is stored (both physically and electronically)

- limit the collection of PII to the minimum amount needed to carry out the functions of the office
- minimize the duplication of PII records
- prohibit unauthorized transfer of PII records to personal devices
- when unattended, physical records containing PII should be kept in locked, unmarked cabinets or areas only accessible to authorized employees.
- departments and authorities should only accept or send faxes of personal information when both the sending and receiving points are known to be located in a locked area with access limited to authorized employees.
- in electronic form, access to PII records should be password-protected and accessible only to authorized employees
- review the use of social security numbers, replacing with alternative personal identifiers wherever possible

Record Retention Policies

The federal government and the Commonwealth of Pennsylvania have established standards for record retention. The Federal Records Act has been in place since 1950 that sets minimum retention standards for its own records, and the Sarbanes-Oxley Act of 2002 regulates minimum record retention for most publicly held companies. The former was most recently updated in 2014 to give the Archivist of the United States final determination of what constitutes a record, and expanded the law to include electronic records.

In Pennsylvania, the Municipal Records Act of 1968 covers cities of the third class, boroughs, incorporated towns, and townships of the first and second classes, but does not apply to first class or second class cities, which includes Pittsburgh. To assist covered municipalities with compliance, the Pennsylvania Historical and Museum Commission issued a Municipal Records Manual in 2009, listing the retention length of various categories of records based on agency type and clarifying procedures for preserving records of permanent value.

Standardized record retention schedules allow private and public sector entities to regularly destroy old records in a manner that reduces risk and vulnerability from data breaches, as well as, limits liability for unlawful divulgence of information. This is also a cost-effective way of reducing storage and retrieval costs and streamlining productivity.

In the private and public sectors, between three and seven years is generally considered an acceptable default retention length when records are not bound by legal obligations. For example, medical records, union agreements, pension records, or any records referenced in a litigation notice must follow federal and state retention requirements.

Finding: The auditors found that no department has an official record retention policy, with some departments keeping records in perpetuity going back decades. This creates an environment where it is increasingly difficult to track what records are held, where they are held, and if any have gone missing.

As a result of this performance audit, PCSC and I&P began working with the Controller's Office auditors and the city archivist to draft formal retention policies.

City Ordinance No. 19 (2012)

One possible roadblock in the city's creation of retention schedules/policies is Ordinance No. 19 of 2012, which established the Commission on city Archives. Under Section 179C.02, it reads:

(b) No city record shall be disposed of until archive plans are promulgated by the Commission on city Archives.

Finding: City Ordinance No. 19 (2012) restricts the ability of departments to destroy unnecessary records. While this was passed with the intention of creating formal retention schedules, no progress was made until the hiring of a city archivist in 2016, who has undertaken the goal set by that ordinance.

While this ordinance was passed with the intent of preserving the city's cultural and historical artifacts, the auditors believe its language is too broad in scope and requires city departments to preserve virtually every physical and electronic record. This creates an unnecessary burden and potential security vulnerability, and is especially imperative when considering the growing amount of electronic data being stored by I&P.

Finding: I&P has retained all records created since 2011, when the city switched its email client from Microsoft Exchange to Gmail. Eventually, the city's servers will reach its capacity and will need to eliminate old electronic records.

RECOMMENDATION NO. 5:

City Council should amend Ordinance No. 19 of 2012 to provide a pathway towards the destruction of PII records. With the city archivist's consultation, the auditors believe the above provision could be amended to read the following:

(b) No city record shall be disposed of until archive plans are promulgated by the Commission on city Archives unless approved by the city Clerk's Office.

Document Shredding

Generally, city departments and authorities use office shredders to destroy documents. While office shredders may be sufficient for some documents, they do not meet security standards to ensure the information contained on the document cannot be pulled back together by computer or by hand. One instance showing how this can be mishandled comes from the Nassau County Police Department in Long Island, where confidential documents containing names and social security numbers ended up as confetti in a 2012 parade.

Most departments and authorities use a secure shredding and disposal vendor to safely destroy records containing personal information. This service allows sensitive physical documents to be discarded into a locked container, where it is later retrieved and securely destroyed by the vendor.

RECOMMENDATION NO. 6:

When destroying physical records containing PII, departments and authorities should always use a secure shredding and disposal vendor. City Council should adopt this as official policy.

Open Records and Open Data (Right to Know Law)

Because government entities are subject to open records, or the Right to Know Law, they are unique in their obligation to make public certain information that would otherwise be considered private. Since January 1, 2009, the city has been subject to the Commonwealth's Right to Know Law, which considers all records of government agencies to be presumed public unless disclosure is barred by state or federal law or regulation; judicial order; or privilege (e.g., attorney-client or doctor-patient). During litigation, the city Law Department takes broad discretion in redacting this information. Section 708 of the Right to Know Law also lists a wide number of exemptions, many of which are considered PII.

These include, but are not limited to: all or part of a social security number; driver's license number; personal financial information; home, cellular or personal telephone numbers; personal e-mail addresses; employee number or other confidential personal identification number; a spouse's name; marital status, beneficiary or dependent information; the home address of a law enforcement officer or judge; letters of recommendation; performance ratings or reviews; civil service test results; employment applications of an individual not hired; written performance criticisms; legal grievance materials; disciplinary documentation; academic transcripts.

Finding: The auditors found that most departments have a Right to Know designated employee who is responsible for processing requests for information.

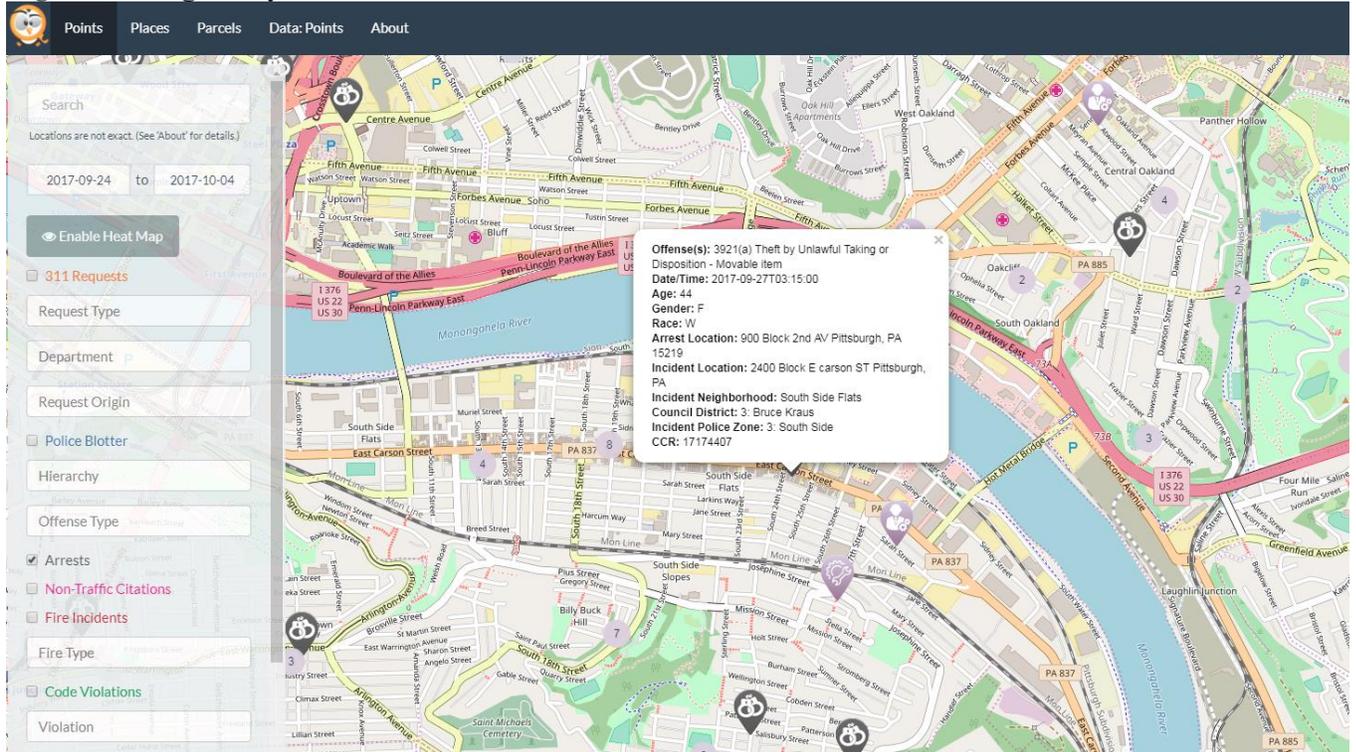
RECOMMEDATION NO. 7:

Having a Right to Know designated employee is a good practice and should continue throughout all city departments/authorities.

While there is a formal process for requesting public records, in recent years the city has taken steps to make data commonly requested available online for public use. Burgh's Eye View is a web application built by I&P that overlays data such as 311 requests, police calls, and code violations onto a map of the city. While the general location of a request or incident is pinpointed on the map, no PII is divulged. For example, an arrest will only list the age, gender, and race alongside the location and offense.

A recent addition to the website, Parcels, makes available the location of properties that are city-owned, delinquent, or part of a tax abatement program, and do not list owner information. However, the external link to that information takes the user to the Allegheny County Real Estate Portal, where owner names and addresses are generally listed. Figure 1 is an example of an arrest report that can be found on Burgh's Eye View.

Figure 1 Burgh's Eye View Screen Shot



RECOMMENDATION NO. 8:

City Council and authorities should develop written record retention policies based on classification of records kept by each city department/authority. This should be done in collaboration with the City Archivist and Law Department to identify records of permanent historical value as well as legally binding documents (e.g., medical records, union agreements, pension records, litigation records, etc.).

RECOMMENDATION NO. 9:

After retention schedules are developed and approved, city departments and authorities should review all current holdings, whether on site or held elsewhere, and securely destroy any records being stored beyond expiration dates. City departments and authorities should then proceed with a regular records purge, archive, and destroy process.

Electronic PII Security

Given the impetus to digitize paper records in the public sector, cyber security is an increasingly pressing concern for municipalities that handle PII.

The majority of city employee information resides in JD Edwards, an enterprise resource planning (ERP) system. An ERP is software that allows an organization to use integrated applications to manage functions related to technology, services and human resources. The physical hardware, including its servers, are housed and maintained by the county, and the city pays a user maintenance fee to access the software. There is a dedicated network link between the city and county, with each maintaining their own security.

Any electronic documents that would contain PII on the city network are kept in shared network folders. An employee's access to shared folders is determined by access control lists that are set by each department. No employee, regardless of seniority, can request a change to their own access privileges. While I&P administrators do not have access to any applications that might store PII, they do have access to any information stored on system disks. All system administrators are fingerprinted and undergo a background check by Allegheny County Police to further safeguard this information.

Finding: Currently, when an employee leaves the city, only PCSC and that employee's supervisor is made aware. User accounts, and any PII contained on them, may remain dormant indefinitely, until I&P is otherwise notified.

RECOMMENDATION NO. 10:

A formal user termination procedure should be established between PCSC and I&P so when an employee leaves the city their account is immediately disabled. If possible, exiting employees should be given the option of providing a forwarding email to send future communications.

Finding: I&P has a solid grasp of the challenges government information technology departments face in protecting PII today.

In managing its own data, I&P wipes clean old hard drives using the federal government standard of a 7-pass erase and are physically drilled out before disposal. User passwords expire every six months, and I&P utilizes virtual desktop infrastructure (VDI) to help quarantine potential threats that prevent viruses from spreading across the network. In addition, a security engineer is always on staff to coordinate, design, and implement new and existing security initiatives to maintain and improve network integrity. These policies should continue.

When dealing with third party vendors, contracts almost always require:

- the city to be notified of any breaches of city data
- city data to be stored and transferred in an encrypted format

- services to adhere to city username and password requirements
- security architecture system that allows for the designation of a security administrator
- vendors for cloud-based systems to have and maintain appropriate certifications
- the provider to perform periodic security audits and submit results to the city
- city data to remain in the United States
- the city to be the proprietary owner of all data
- data to be securely destroyed.

Finding: It appears that information is secure against external threats. However, there could be improvements against the theft of PII from those who already have access to the network.

For example, a tactic called “pod slurping” involves using an external storage device to illicitly download large amounts of confidential data in a short period of time. Though instances are rare, any comprehensive PII protection strategy should consider all points of vulnerability.

Following a 2015 data breach, the federal Office of Personnel Management (OPM) took steps to improve cybersecurity that included two-factor login authentication. In addition, endpoint security software was installed that allowed the office to see all devices connected to the network and monitor all data moving in and out of the system. Such measures should be considered by I&P as further preventative security.

RECOMMENDATION NO. 11:

I&P should develop and maintain a detailed inventory of all PII held, review shared network access rules, examine any areas where PII could be compromised, and identify preventative measures that can be taken to safeguard against internal data theft, including endpoint security software.

Finding: There is no official policy in place that guides the actions and procedures the city should take in the event of a data breach. While the city is subject to Pennsylvania’s 2005 Breach of Personal Information Act, technology has advanced substantially since then, and the city should formalize a policy that reflects its current needs.

RECOMMENDATION NO. 12:

I&P’s security engineer should develop a data breach response policy that includes reporting the breach to the appropriate senior management, strategies for containing the breach, assessing the need to notify affected parties, and documenting actions taken at each stage to review the incident and prevent future breaches. This policy should apply to all city departments and authorities that handle PII.

Employee PII Awareness and Training

For any comprehensive PII protection strategy to function effectively, it is essential that all employees are aware of what PII is, what policies and procedures are in place, how to avoid compromising that information, and who to report future incidents to.

Finding: PII awareness among city employees is low, and there is no formal strategy to educate new and existing employees on how to handle PII or avoid its compromise.

Finding: City employees have been targeted by various phishing scams in an effort to solicit private information.

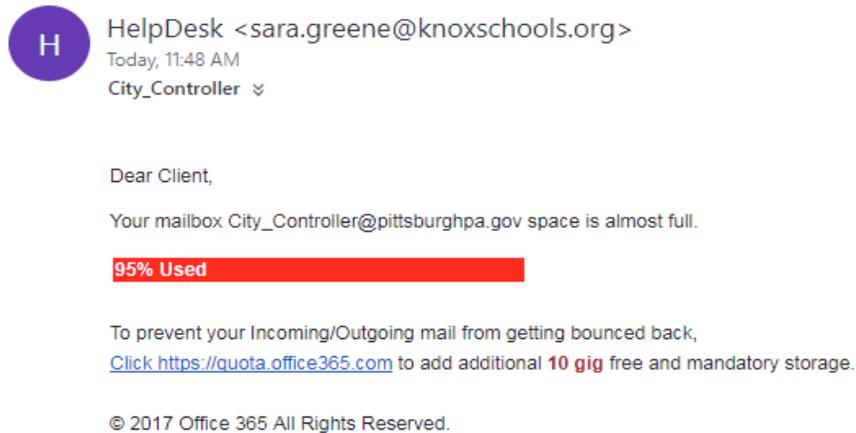
One example, shown below, prompts the user to visit an external site where sensitive login and password information is solicited under the guise of receiving a work quote. These types of scams vary in complexity and sophistication, but any could be used to gain access to an employee's system account and retrieve PII. Examples are shown in Figures 2 and 3 below.

Figure 2 Phishing Scam Example



Figure 3 City Employee Email Scam

Increase Your Mailbox Quota



RECOMMENDATION NO. 13

The city should conduct ongoing PII awareness training to new and existing employees, with I&P taking a prominent role. This should include what PII is and the risks involved in its collection, storage, transmission, and disposal. The city should also educate employees about the legal implications of violating personal information at any point of employment or post-employment, and methods for preventing such violations, including the ability to encrypt city emails and avoiding communications containing phishing scams.

Finding: The city email client, Microsoft 365, enables anyone sending an email to have its contents encrypted by using “ENCRYPT.” at the beginning of a subject line. This protects confidential information from being intercepted by adding another level of security to communications. However, the auditors found little awareness of this feature among the city employees they met with, and the city does not take an active role in educating or training employees about what PII is or how to keep it secured.

RECOMMENDATION NO. 14:

The city should require an encryption procedure when transmitting PII on the city network (including through email) or onto an external storage device.

Finding: The Sports and Exhibition Authority requires third party vendors managing sensitive personal information to have cyber insurance. This type of insurance protects a private or public entity from a set amount in damages resulting from compromised technology.

Cyber insurance often provides services such as crisis management, security breach notification, and data restoration. Given the vast amount of personal data they hold, and the high

costs of dealing with a cyber-attack that compromises that information, a growing number of municipalities are embracing cyber insurance to protect citizens' personal information.

RECOMMENDATION NO. 15:

The city should consider the purchase of cyber security insurance, and/or require contractors to have cyber security insurance when managing personally identifiable information.