

Information Security Policy

Scope: CITYWIDE

Policy Contact

Information Technology Department
(916)808-7111
ithelpdesk@cityofsacramento.org

Table of Contents

1. Purpose	2
2. Roles and Responsibilities	2
3. Policy Directive	4
4. Data Access Control	6
5. Information Security Awareness and Training	7
6. Outside Party Security	8
7. Guidelines for Security of Data in Hardcopy Format	8
8. Network Security	8
9. Encryption	9
10. Viruses and Malicious Software	9
11. Applications and Systems Development	10
12. Cloud Approval and Governance	10
13. Contingency Planning	11
14. End Users Privacy	11
15. Customer Privacy	12
16. Management Support for Information Security	12
17. Policy Compliance	12
18. Reporting Policy Violations	12
19. Definitions	13
Charter Officer Review and Acknowledgement	16

Related Regulatory References

National Institute of Standards and Technology (NIST) Special Publication 800.X
PCI Policy

Reviewed/Effective:

May 1, 2023

1. Purpose

It is the policy of the City of Sacramento (“City”) to protect the confidentiality, integrity, and availability of the City’s data while meeting the open, information-sharing needs of its constituents and performing government services.

The policy serves as an administrative control to manage the risks to information technology resources (“ITRs”) from deliberate acts of sabotage or ill-intent, natural disasters, and accidents caused by humans and non-humans.

2. Roles and Responsibilities

A. Charter Officers and Department Directors

Charter Officers and Department Directors are responsible for:

- i. Ensuring that end users within their respective departments receive and review this policy through the City’s Learning Management System (“LMS”);
- ii. Monitoring end user compliance with this policy;
- iii. Designating an Information Security Liaison (“ISL”) to be the primary point of contact responsible for department compliance with this policy and coordination with the City’s Information Technology (“IT”) Department;
- iv. Causing the review of their departmental information security practices annually or as needed, to ensure conformance with this policy and compliance with information security standards and guidelines; and
- v. Ensuring that a Business Continuity Plan (“BCP”) and Disaster Recovery Plan (“DRP”) is in place for their business.

B. Chief Information Officer (“CIO”)

The Chief Information Officer is responsible for:

- i. Managing and enforcing this policy;
- ii. Appointing an Information Security Officer (“ISO”);
- iii. Overseeing personnel with significant responsibilities such as ISLs for the City’s information security and ensuring such personnel are adequately trained;
- iv. Assisting persons at the level of division manager and above with their security responsibilities to ensure personnel with access to confidential data are adequately trained;
- v. Updating this policy as needed; and
- vi. Performing such other duties necessary to implement this policy.

C. Information Security Officer (“ISO”)

Information Security Officer is responsible for:

- i. Implementing and managing, under the direction of the CIO, a citywide Information Security Program that contains administrative, technical, and physical safeguards that comply with this policy and are designed to protect data and ITRs as required by applicable laws and regulations;
- ii. Implementing, coordinating, and maintaining operating procedures, guidelines, and standards governing information security, under the direction of the CIO;
- iii. Ensuring the City is in compliance with applicable information security laws and regulations by consulting and coordinating with subject matter experts;
- iv. Periodically assessing the City’s risk for unauthorized:
 - a. access to data and ITRs;
 - b. use, disclosure, modification, or destruction of data; and
 - c. use, disruption, modification, or destruction of ITRs;
- v. Assisting the CIO with updating this policy to provide adequate information security for networks, facilities, and ITRs including:
 - a. periodically testing and evaluating the effectiveness of this policy; and
 - b. establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in this policy;
- vi. Providing appropriate information security awareness training to end users;
- vii. Overseeing and providing training to other personnel that have information security responsibilities;
- viii. Establishing and maintaining a process for detecting, reporting, and responding to information security incidents;
- ix. Guiding the Information Security Steering Committee (ISSC) in addressing City and departmental information security needs and concerns.

D. Information Security Liaison (“ISL”)

ISLs are responsible for:

- i. Being a City department’s primary point of contact responsible for department compliance with this policy in coordination with the IT Department; and
- ii. Reviewing the department’s security practices periodically and assessing department’s information security needs.

E. Information Security Steering Committee (“ISSC”)

ISSC is responsible for:

- i. Evaluating City information security policies, procedures, and operations to identify potential areas of vulnerability and risk and assist with the strategic direction the City’s information security.

F. End Users

End users are responsible for:

- i. Reviewing and acknowledging this policy via the City's LMS;
- ii. Complying with this policy;
- iii. Handling data based on its classification in accordance with this policy;
- iv. Obtaining proper authorization prior to accessing ITRs; and
- v. Reporting anomalies or suspicious ITR-related behavior to the IT Help Desk at ITHelpDesk@cityofsacramento.org.

G. Data Owners

Data owners (this role is usually done by an IT employee unless otherwise specified) are responsible for:

- i. Categorizing the data according to the classification standard set forth by this policy; and
- ii. Assigning a data custodian responsible for maintaining and protecting the data.

3. Policy Directive

A. Copying Software

End users shall not copy software provided by the City to any storage media, transfer such software to another computer, or disclose such software to outside parties without advance coordination with the IT Department to determine if this activity is allowed under the appropriate end user license agreement or if additional software licenses would need to be procured. Ordinary backup copies are an authorized exception to this policy.

B. Data Classification and Handling

To adequately protect ITRs, data must be handled in accordance with its classification based on its sensitivity and criticality to operations. The City's data, whether in electronic or physical form, can be classified as follows:

- i. **Confidential (Level 1)**: Access, storage, and transmission of confidential data should be handled in accordance with subsection b, below.
 - a. **Confidential Classification Defined**: Data may be classified as confidential based on risk criteria, including whether disclosure to persons outside of the City is governed by applicable laws and regulations designed to protect it; and if unauthorized use, access, disclosure, acquisition, modification, loss,

or deletion could result in legal action, financial loss, severe damage to the City's reputation, its employees, or customers.

- b. **Protection:** Data categorized as Level 1 should be protected throughout its entire life cycle, from origination to destruction. End users are strongly encouraged to protect Level 1 information using the principles of least privileges and need-to-know. In addition, end users should protect Level 1 data during its transmission across the Internet or public networks in a manner that ensures its confidentiality and integrity between a sender and a recipient. Unless encrypted, email is not considered a secure way to transmit data.
- c. **Examples of Level 1 information include:**
 1. Passwords or credentials that grant access to critical and business data
 2. PINs (Personal Identification Numbers)
 3. Birth date combined with last four digits of SSN (Social Security Number) and name; credit card numbers with cardholder name
 4. Tax ID with name
 5. Driver's license and number, state identification card and number, and other forms of national or international identification (such as passports, visas, etc.) in combination with name
 6. Electronically protected health information (ePHI)
 7. Medical records related to an individual
 8. Psychological counseling records related to an individual
 9. Bank account or credit/debit card information in combination with any required security code, access code, or password that would permit access to an individual's financial account
 10. Biometric information
 11. Electronic or digitized signatures
 12. Private key (digital certificate)
 13. Law enforcement personnel records
 14. Criminal background check results
 15. Attorney-client communications and attorney work-product
 16. Personally Identifiable Information (PII)
- ii. **Internal Use (Level 2):** Access, storage, and transmission of internal use information should be handled in accordance with subsection b, below.
 - a. **Internal Classification Defined:** Data may be classified as internal use if the data is strictly accessible to internal City personnel or internal employees who are granted access. This might include data that is intended solely for use within the City and limited to those with a business need-to know, whether or not the data is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws.

- b. Protection: Data categorized as Level 2 requires moderate protection. End users must protect Level 2 information using the principles of least privileges and need-to-know.
 - c. Examples of Level 2 information include:
 - 1. Internal Correspondence
 - Emails
 - Chat Messages
 - Memos
 - Voicemail
 - 2. Data in ITR's
 - Software licensing information
 - Vulnerability/security information
 - Service Desk ticketing system data
 - IT asset management data
 - System logs
 - Telecommunication Circuits
 - Network Systems Diagrams
 - 3. Infrastructure Plans
 - Building Plans
 - City plans
 - Utility plans
- iii. **Public (Level 3)**: Access, storage, and transmission of internal use information should be handled in accordance with subsection b, below.
- a. Public Classification Defined: Data that is publicly known or available or widely available in the specific industry.
 - b. Protection: Data at this level requires no specific protective measures but may be subject to appropriate review or disclosure procedures at the discretion of the City to mitigate potential risks.
 - c. Examples of Level 3 information include:
 - 1. Publicly available data and information
 - City's Public Website
 - Open DataPortal

4. Data Access Control

Data owners are responsible for determining and approving the necessity of an end user's access to the data. Data owners shall compose access control standards based on the principles of need-to-know and least privilege. Data owners should follow separation of duties principles when assigning tasks to end users when the task involves restricted or essential ITRs. The IT Department shall develop and implement authentication controls for access to ITRs that access or store confidential data. The authentication controls shall be unique to

each individual and may not be shared unless authorized by appropriate City management in writing with a business justification. Such written authorization shall be provided to the Information Security Officer upon request.

End users are responsible for the protection and security of ITRs accessed while logged on to those resources from outside the City's network. End users shall not misuse ITRs and shall protect such ITRs, to the extent reasonably possible, from misuse. Misuse includes, but is not limited to, theft, unauthorized access and data transfers, fraudulent manipulation or alteration of data, attempts to circumvent the security controls, and any activity that could compromise the confidentiality, integrity, or availability of data.

End users separated from the City are expected to keep confidential any knowledge of ITRs obtained or accessed while employed by the City. Access to ITRs shall be revoked by the department that has primary responsibility for the applicable system upon the termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by the City. Access shall be revoked as soon as possible and shall not exceed (3) business days after access is no longer required.

End users shall immediately notify the IT Department and data owners if confidential information is lost, disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties.

The City reserves the right to temporarily or permanently suspend, block, or restrict access to ITRs when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of City resources and data.

Browsing, altering, or accessing electronic messages or stored files in another end user's account, computer, or other electronic storage device is prohibited, even when such accounts or files are not password protected unless specifically authorized by the end user for City business reasons.

Only hardware or software that has been approved by the IT Department may be connected to the City's computer systems and data and voice networks. However, peripheral devices (i.e., headphones, keyboards, monitors, mouse, speakers, portable data storage devices/media etc.) may be connected without seeking IT Department approval. If the peripheral device stores data, then that data must be maintained in accordance with its classification (see section 3.B.) and proper security measures should be taken to prevent and avoid infection by malware.

5. Information Security Awareness and Training

All end users shall complete an approved information security awareness training course at least annually or as necessary for their job function or as needed per applicable laws and regulations. New end users that are employees shall complete the course within 30 days of employment.

The Information Security Office shall conduct annual security awareness and training. Training may include phishing simulations and other related matters. If the Information Security Office determines through its assessment that an end user lacks the knowledge or requisite skills to properly protect ITRs, the Information Security Officer may require the end user to take the appropriate training.

6. Outside Party Security

Generally, City confidential and internal data may not be disclosed to outside parties. However, outside parties may be given access to City internal data only when a demonstrable need-to-know basis exists, and the outside party agrees to abide by a non-disclosure agreement and the following information security requirements:

- A. As a condition of gaining access to the City's computer network, every outside party must secure its own connected systems in a manner consistent with this policy.
- B. The City reserves the right to audit the security measures in effect on outside party-connected systems without prior warning.
- C. The City also reserves the right to immediately terminate network connections with all outside party systems not complying with this policy.
- D. The outside party shall immediately notify the City if City confidential or internal data is lost, disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties.

7. Guidelines for Security of Data in Hardcopy Format

If it can be easily or conveniently accomplished, end users should physically restrict access to their work areas containing confidential data to protect them from unauthorized disclosure and should position their computer screens such that unauthorized persons cannot see the confidential data.

8. Network Security

Unless otherwise stated, all security measures will be implemented by the IT Department.

All connections between City internal networks and the Internet or any other publicly accessible computer network must include an approved firewall or related access control system. The privileges permitted through this firewall or related access control system must be based on business needs and must be defined in an access control standard.

City computers that are permanently or intermittently connected to internal computer networks must have a secure access control system approved by the Information Technology Department. Regardless of the network connections, all stand-alone computers handling confidential data must also employ an approved secure access control system.

End users working with all other types of computers must sign into their computers and after a period of no activity the screen will go blank until the end user credentials are entered again. Multi-user systems throughout the City must employ automatic log-off systems that automatically terminate an end user's session after a defined period of inactivity.

All in-bound session connections to the City's computers from external networks must be protected with multifactor authentication. End users with personal computers connecting to City internal network resources should maintain their computers up to date with the latest security patches and have an antimalware checking system enabled. When using City computers on City premises, end users must not establish connections with external networks, including but not limited to Internet service providers, detected wireless networks not provided by the City, etc. The Guest Wi-Fi network is considered an external network and should not be used while conducting City business.

City computers or networks may be connected to outside party computers or networks only after the Information Technology Department has determined that the combined systems will be compliant with the City's security requirements.

9. Encryption

Whenever confidential data is sent over a public computer network like the Internet or stored on removable media, IT strongly recommends that encryption methods authorized by IT be used to protect it. However, end users should be aware that encryption of certain confidential data may be required by law or regulatory requirements. End users should consult IT and the City Attorney's Office to determine if the data must be encrypted pursuant to a law or regulation. If an end user fails to encrypt confidential data and such failure is due to extreme carelessness or malicious exploitation of the data, this failure is subject to discipline. Non-City computer systems storing confidential data should be encrypted as well. Please refer to the City's Data Classification Standard for more information.

Encryption keys will be managed and stored by the key custodian in a secured central repository. Key management involves administering the full lifecycle of cryptographic keys and protecting them from loss or misuse. The lifecycle includes generating, using, storing, archiving, and deleting of keys. Protection of the encryption keys includes limiting access to the keys physically, logically, and through role-based access.

10. Viruses and Malicious Software

The IT Department must approve and install malicious software detection systems on all City servers and devices. These systems are used for many purposes including checking files for viruses before execution or usage. End users must not turn off or disable malicious software detection systems.

11. Applications and Systems Development

ITRs that have been designated production systems have special security requirements. A production system is a system that is regularly used to process data critical to the City's business. Although a production system may be physically situated anywhere, the production system designation is assigned by the Assistant IT Director.

All software developed in-house that runs on production systems must be developed according to the Information Technology Department's systems development methodology ("SDM"). This methodology must ensure that the software will be adequately documented and tested before it is used for critical City data. The SDM also must ensure that production systems include adequate control measures. Production systems also must have designated data owners and key custodians for the critical data they process. Information Security Officer must perform periodic risk assessments of production systems to determine whether the controls employed are adequate. All production systems must have an access control system to restrict who can access the system and restrict the privileges available to these end users. A designated access control administrator who is not a regular end user on the system must be assigned for all production systems by the system owner.

Where resources permit, there must be a separation between the production, development, and test environments. Where these distinctions have been established and as resources permit, development and test employee(s) must not be permitted to have access to production systems. All production software testing must proceed with sanitized data where confidential data is replaced with dummy data. All security fixes provided by software vendors must go through the systems development methodology testing process and must be promptly installed. The formal and documented City change control process must be used to restrict and approve changes to production systems. All application program-based access paths other than the approved end user access paths must be deleted or disabled before software is moved into production.

All production software development and software maintenance activities performed by in-house employees must adhere to the Information Technology Department's policies, standards, procedures, and other systems development conventions. These conventions include proper testing, training, and documentation.

12. Cloud Approval and Governance

End users must not use cloud computing services, open cloud services accounts, or enter into cloud service contracts for the storage, manipulation, or exchange of City-related communications or City-owned data without the approval of the Information Technology Department. Personal cloud services accounts such as Google Drive, OneDrive, etc. may not be used for the storage, manipulation, or exchange of City-business related communications or City-owned data or exchange of City-business related communications or City-owned data.

All outside-party processing (cloud) vendors must be pre-approved by the Information Technology Department. The Information Technology Department must certify that security, privacy, and all other IT management requirements will be adequately addressed by the cloud computing vendor.

Additional control requirements adopted as part of cloud service arrangements must be formally adopted into the City internal control framework.

In establishing login credentials for outside-party (cloud) services, end users must comply with existing City security requirements for secure passwords and must notify their manager and IT of the details of the account and the types of data being stored. An exception to this policy is made when the Information Technology Department establishes and assigns these accounts.

Personally identifiable information must not be stored in outside-party (cloud) environments that are located in foreign countries.

13. Contingency Planning

Department Directors, in conjunction with the Office of Emergency Services and the Department of Information Technology, must prepare, annually update, and regularly test each of the following:

- A. Business Continuity Plan that provides procedures for sustaining essential business operations while recovering from a significant disruption;
- B. Cyber Incident Response Plan that focuses on information security responses to incidents affecting systems or networks;
- C. IT Contingency Plan for recovering major application or general system support that addresses IT system disruptions; and
- D. Disaster Recovery Plan that specifies how alternative facilities (offices, telephones, copiers, etc.) will be provided so City employees can continue operations in the event of a business interruption. The DRP applies to major, usually physical, disruptions to service that deny access to the primary facility infrastructure for an extended period.

14. End Users Privacy

End users have no reasonable expectation of privacy when using ITRs while working for the City, excepting applicable laws. To manage systems and enforce security, the City may log, review, and otherwise utilize any data stored on or passing through its systems. The City may capture end user activity such as telephone numbers dialed, websites visited, etc. All City ITRs are City property and may be monitored. The City retains the right to remove from its ITRs any material it views as offensive or potentially illegal.

15. Customer Privacy

The City does not collect any data that is unnecessary for business purposes. The City does not collect data from outside parties, such as customers, unless these parties are notified about the collection activities before they occur.

A wide variety of parties have entrusted their information to the City of Sacramento for business purposes, and all end users of the City must do their best to safeguard the privacy and security of this data. Customer account data is confidential and access must be strictly limited based on the business need for such access. Customer account data must not be distributed to outside parties without advance written authorization by the customer.

16. Management Support for Information Security

Guidance, direction, and authority for Information Security activities for the City fall under IT, Information Security Office. The Information Security Office will provide direction and expertise to ensure the City's data is protected. This responsibility includes consideration of the confidentiality, integrity and availability of both data and ITRs that manage information. The IT Department will act as a liaison for all information security matters with all City departments and IT service providers and must be the focal point for all information security activities throughout the City.

17. Policy Compliance

At the City's sole discretion, end users who violate this policy may be subject to disciplinary action following established City channels for disciplinary matters, applicable breach of contract remedies, cessation of volunteer services, or other appropriate legal remedies. Such actions must be administered in a manner consistent with the terms of the applicable collective bargaining agreement and Human Resources/Labor Relations policies and practices. Contract employees who violate the requirements of the policy may be subject to appropriate disciplinary actions as defined by their organization's policies. End users that are consultants or vendors who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the City. The City may also refer suspected violations to appropriate law enforcement agencies.

18. Reporting Policy Violations

All suspected system intrusions, virus infestations, and other conditions that might jeopardize the City's data or ITRs must be immediately reported to the IT Service Desk for investigation.

If an end user believes that a violation of this policy has occurred, they should either coordinate with an appropriate department supervisor or manager and relay the data to the Information Security Office at iso@cityofsacramento.org or open a ticket for the Information Security Office with the IT Service Desk.

An Information Technology Department supervisor or manager shall review the reported violation, contact the CIO, and determine if additional City offices should be contacted.

19. Definitions

Access	The privilege or assigned permission to use electronic data or ITRs in some manner.
Access Controls	A process for limiting access to an ITR or to physical or virtual resources. In computing, access control is a process by which end users are granted access and certain privileges to systems, resources or information.
Account	A level of privileged access that is created for ITRs.
Authentication Controls	Any process by which a system verifies the identity of an end-user who wishes to access the system (e.g., a username and password, token, or biometric).
Business Continuity Plan (“BCP”)	The documentation of a predetermined set of instructions or procedures that describe how an organization’s mission/business processes will be sustained during and after a significant disruption. Source:NIST https://csrc.nist.gov/glossary/term/business_continuity_plan
Charter Officers	Officers appointed under the City’s Charter or designees.
Chief Information Officer (“CIO”)	The director of the City’s Information Technology Department or designee.
Computer-related positions of trust	Information technology employees who have access to systems storing or processing Level 1 classified data per the data classification standard.
Computer systems	A set of integrated devices that takes in, produces, processes, and stores data.
Customer	People or end users who receive services from the City.
Customer account information	Data about a customer such as name, address, account numbers, billing data, or other similar data.
Data	Factual information that is used as a basis for reasoning, discussion, or calculation.
Data classification standard	The process of organizing data by relevant categories so that it may be used and protected more efficiently.
Data owner	The City department or outside party in charge of, has administrative control over, and is responsible and accountable for a particular set of data.
Department Director	The director, chief, or top managerial authority for a City department or designee.
Department of Information Technology (“IT”)	The City’s Department of Information Technology.
Development environment	The set of processes and programming tools used to create a program or software.

Disaster Recovery Plan (“DRP”)	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. Source: NIST https://csrc.nist.gov/glossary/term/disaster_recovery_plan
End users	City employees, administrators, contractors, consultants, vendors, volunteers, temporary agency employees, student interns, or any other person who uses or is provided access to Information Technology Resources in accordance with this policy.
Emergency	A serious, unexpected, and often urgent situation resulting in a technological system outage that impacts end-users or technology infrastructure requiring immediate action for resolution.
Guidelines	Recommended actions or industry best practices that should be used to ensure compliance with the policy.
Home directory	The directory or location that serves as an exclusive electronic repository for an end user's files and folders.
Information Technology Resources (“ITR”)	City-owned leased, or controlled computers, servers, network and radio infrastructure, current or future connectivity solutions, peripherals, technological assets and related equipment, software, hardware, and mobile applications.
Information security	The protection of data and associated information technology resources from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality and integrity, and secure the availability of such data.
Information Security Officer (“ISO”)	The individual assigned by the CIO to be the Department of Information Technology's Information Security Officer responsible for establishing and maintaining IT security operating procedures, guidelines, and control techniques to properly address all applicable requirements, subject to the Chief Information Officer's approval, or designee.
Information Security Program	A documented set of information security policies, procedures, guidelines, and standards that will ensure the confidentiality, integrity, and availability of information technology resources.
Information security incidents	Events that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed.
Key custodian	The City employee responsible for creating, altering, recovering, rotating, distributing, and maintaining encryption keys.
Learning Management System (LMS)	A software system for the administration, documentation, tracking, reporting and delivery of educational courses,

	policies, training programs, or learning and development programs.
Need-to-know	An individual has a City-business related need-to-know certain data to conduct City duties.
Outside Party/Parties	External parties with which the City does business with such as service providers, other government entities, corporations, non-profit associations, contractors, individuals, etc.
Personally Identifiable Information (“PII”)	Data that could potentially identify a specific individual, or any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data.
Principle of least privileges	The practice of limiting access rights for end users to the bare minimum permissions they need to perform their work.
Production environment	A setting where the program or software and other products are put into operation for their intended uses by end-users.
Separation of duties	The concept of having more than one person required to complete a task. For example, the requestor can’t also be the approver. The separation is when more than one person shares a task and is an internal control intended to prevent fraud and error.
System owner	The City department or outside party in charge of, has administrative control, and is responsible and accountable for an information system.
Stand-alone computers	A computer that is used on its own without requiring a connection to a local area network or wide area network. Although it may be connected to a network, it is still a stand-alone personal computer if the network connection is not mandatory for its general use
Test environment	An environment of software or hardware that is used for testing different scenarios to ensure proper functionality of the program or software.



Charter Officer Review and Acknowledgement Information Security Policy

(Signature by all charter officers is not a requirement for policy adoption)



[Howard Chan \(Apr 25, 2023 18:41 PDT\)](#)

City Manager Apr 25, 2023



[Susana Alcalá Wood \(May 4, 2023 09:07 PDT\)](#)

City Attorney May 4, 2023

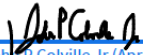


City Clerk Apr 26, 2023



[Jorge Oseguera \(Apr 26, 2023 11:19 PDT\)](#)

City Auditor Apr 26, 2023



[John P. Colville Jr \(Apr 25, 2023 18:57 PDT\)](#)

City Treasurer Apr 25, 2023