City of Santa Ana Administrative Policies and Procedures	City Manager's Authorization	
Subject **REMOTE ACCESS POLICY**	Date 10/10/2023	Number IT-04

1. Purpose

The purpose of this policy is to establish guidelines and procedures for secure and authorized remote access to the City of Santa Ana's internal network and resources. This policy aims to protect the City's sensitive data, maintain the confidentiality and integrity of information, and ensure compliance with applicable laws and regulations. This policy document serves as a revised version of the Remote Access Policy implemented in September 2006. It has been updated to align with current organizational needs and industry best practices.

2. Scope

This policy applies to all employees, contractors, consultants, and any other individuals granted remote access privileges to Santa Ana's network and resources. It supersedes the previous Remote Access Policy in its entirety and is applicable beginning October 10, 2023. All employees who request remote access to the City's network are expected to familiarize themselves with this revised policy and adhere to its guidelines.

3. Authorized Remote Access

1. Eligibility

Remote access privileges shall only be granted to authorized personnel who require such access to perform their job duties effectively, and may be revoked by the City at any time. Approval for remote access shall be obtained through the appropriate channels and in accordance with established procedures.

2. Authentication

All remote access sessions must be authenticated using strong, unique, and regularly updated credentials. Passwords must meet minimum complexity as defined by the City's Password Policy, and multi-factor authentication (MFA) shall be implemented using access methods approved by the City's Information Technology (IT) Department, which may require the use of a personal device, such as a cell phone, for authentication purposes only.

3. Access Control

Access to specific resources and systems during remote sessions shall be granted based on the principle of least privilege. Users shall only be granted access to the resources necessary to perform their job responsibilities. Access rights shall be reviewed periodically and revoked promptly upon termination of employment or change in role.

4. Service Ownership

The remote access service is owned by the City of Santa Ana and the contents traveling electronically through it may be monitored, examined, saved, read, transcribed, stored, or retransmitted in the course of business without the consent of the user. Remote access users should have no expectations of privacy for data transferred using the service.

5. Secure Connections

Remote access sessions are allowed through established secure and encrypted connections, such as virtual private networks (VPNs) or other approved methods. Open, unsecured, public networks, or Wi-Fi connections should be avoided whenever possible. Use caution when connecting to any unfamiliar network.

4. Security Measures

1. Device Security

Devices used for remote access, including personal computers and mobile devices, must adhere to the City of Santa Ana's approved security standards. This includes maintaining up-to-date operating systems, antivirus software, and regular installation of security patches and updates. The IT Department maintains the right to approve or deny access to specific devices.

2. Data Protection

All sensitive data accessed remotely must be protected and treated in accordance with the City of Santa Ana's Data Protection and Privacy Policy. City IT provided encryption mechanisms should be used to safeguard data in transit and at rest.

3. Prohibited Activities

The following activities are strictly prohibited during remote access sessions:

3.1. Sharing or disclosing remote access credentials with unauthorized individuals.

3.2. Unauthorized access to, use of, or modification of data, systems, or resources.

3.3. Installation of unauthorized software or applications.

3.4. Introduction of malicious software, viruses, or other harmful content.

3.5. Violation of applicable laws, regulations, or contractual obligations.

5. Policy Compliance, Enforcement, Reporting, and Incident Response

1. Security Incidents

Any suspected or actual security incidents or breaches related to remote access must be reported immediately to the designated IT or security personnel. The incident response procedures defined by the City of Santa Ana shall be followed to investigate and mitigate the incident.

2. Loss or Theft of Devices

Any loss or theft of devices used for remote access must be reported promptly to the IT department. Measures such as remote data wipe or device deauthorization shall be initiated to mitigate the risk of unauthorized access.

3. Compliance and Monitoring

Periodic audits and compliance assessments shall be conducted to ensure adherence to this Remote Access Policy. Monitoring of remote access sessions is regularly performed to detect and prevent unauthorized activities or security threats. Users should be aware that their remote access activities may be logged and monitored.

4. Policy Review and Updates

This Remote Access Policy shall be reviewed on a regular basis to reflect changes in technology, regulatory requirements, or organizational needs.

5. Policy Violations and Consequences

Failure to comply with this Remote Access Policy may result in disciplinary action, up to and including termination of employment or contract.

6. Document History

- Version 1.0: 9/1/2006 – Initial policy implementation.
- Version 2.0: 10/10/2023 – Revised policy replacing Remote Access Policy implemented 9/1/2006.