*** * * * PUBLIC NOTICE * * * ***

NOTICE OF A CITY COUNCIL REGULAR SESSION IMMEDIATELY FOLLOWING A WORKSHOP SESSION OF THE CITY OF CORINTH
Thursday, February 20, 2020, 5:45P.M.
CITY HALL - 3300 CORINTH PARKWAY

CALL TO ORDER:

WORKSHOP BUSINESS AGENDA

1. Receive a report, hold a discussion, and give staff direction on the Water and Wastewater Rates.

2. Receive a Presentation and hold a discussion regarding the Lake Cities Fire Department/Joint Lake Cities Council Meeting.

3. Discuss Regular Meeting Items on Regular Session Agenda, including the consideration of closed session items as set forth in the Closed Session agenda items below.

ADJOURN WORKSHOP SESSION

***NOTICE IS HEREBY GIVEN** of a Regular Session of the Corinth City Council to be held at Corinth City Hall located at 3300 Corinth Parkway, Corinth, Texas. The agenda is as follows:

CALL TO ORDER, INVOCATION, PLEDGE OF ALLEGIANCE & TEXAS PLEDGE:
"Honor the Texas Flag: I pledge allegiance to thee, Texas, one state under God, one and indivisible".

CONSENT AGENDA
All matters listed under the Consent Agenda are considered to be routine and will be enacted in one motion. Should the Mayor, a Councilmember, or any citizen desire discussion of any Item that Item will be removed from the Consent Agenda and will be considered separately.

1. Consider and act on approval of an Interlocal Agreement with the City of Missouri City for cooperative purchasing.

2. Consider and act on a Resolution reviewing and approving the Technology Services Security Policy for the City of Corinth; and providing an effective date.

3. Consider approval of the DataProse contract renewal and expenditures for bill processing, postage and inserts.

4. Consider and act on a Resolution reviewing and approving the Incident Response Policy and Plan for the City of Corinth and Providing an Effective Date.

CITIZENS COMMENTS
In accordance with the Open Meetings Act, Council is prohibited from acting on or discussing (other than factual responses to specific questions) any items brought before them at this time. Citizen's comments will be limited to 3 minutes. Comments about any of the Council agenda items are appreciated by the Council and may be taken into consideration at this time or during that agenda item. Please complete a Public Input form if you desire to address the City Council. All remarks and questions addressed to the Council shall be addressed to the Council as a whole and not to any individual member thereof. Section 30.041B Code of Ordinance of the City of Corinth.

BUSINESS AGENDA

5. Consider authorzing the city manager to execute a memorandum of agreement between the CIty of Corinth and the Dallas Off-Road Bicycle Association (DORBA), for the use and maintenance of Corinth trails.

6. Consider and act on a request by Classic Mazda Company for an application to the Unified Development Code Section 4.01.15. General Requirements – Section E – 3. Maximum Height, Section E – 4 Maximum Sign Area and E- 5 Maximum Sign Structure Area. The request is to allow certain increases to the monument sign allowed by ordinance requiring City Council approval. The sign being replaced is located at 5000 S. I35E along the I-35E frontage, legally described as Lot 1, Blk A of the Classic Mazda Addition, City of Corinth, Denton County, Texas.

COUNCIL COMMENTS & FUTURE AGENDA ITEMS
The purpose of this section is to allow each councilmember the opportunity to provide general updates and/or comments to fellow councilmembers, the public, and/or staff on any issues or future events. Also, in accordance with Section 30.085 of the Code of Ordinances, at this time, any Councilmember may direct that an item be added as a business item to any future agenda.

CLOSED SESSION
The City Council will convene in such executive or (closed session) to consider any matters regarding any of the above agenda items as well as the following matters pursuant to Chapter 551 of the Texas Government Code.

Section 551.071. (1) Private consultation with its attorney to seek advice about pending or contemplated litigation; and/or settlement offer; and/or (2) a matter in which the duty of the attorney to the government body under the Texas Disciplinary Rules of Professional Conduct of the State of Texas clearly conflicts with chapter 551.

Section 551.072. To deliberate the purchase, exchange, lease or value of real property if deliberation in an open meeting would have a detrimental effect on the position of the governmental body in negotiations with a third person.

Section 551.074. To deliberate the appointment, employment, evaluation, reassignment, duties, discipline, or dismissal of a public officer or employee; or to hear a complaint or charge against an officer or employee.

Section 551.087. To deliberate or discuss regarding commercial or financial information that the governmental body has received from a business prospect that the governmental body seeks to have locate, stay, or expand in or near the territory of the governmental body and with which the governmental body is conducting economic development negotiations; or to deliberate the offer of a financial or other incentive to a business prospect.

a. Discuss potential Economic Development incentives for businesses seeking to locate in Corinth and supporting the TOD.

After discussion of any matters in closed session, any final action or vote taken will be in public by the City Council. City Council shall have the right at any time to seek legal advice in Closed Session from its Attorney on any agenda item, whether posted for Closed Session or not.

RECONVENE IN OPEN SESSION TO TAKE ACTION, IF NECESSARY, ON CLOSED SESSION ITEMS.

ADJOURN:

Posted this 14th day of February, 2020 at 11:30 a.m. on the bulletin board at Corinth City Hall.

Kimberly Pence
Kimberly Pence, City Secretary
City of Corinth, Texas

WORKSHOP BUSINESS ITEM 1.

City Council Regular and Workshop Session

Meeting Date:	02/20/2020
Title:	Water Rate Study
Submitted For:	Lee Ann Bunselmeyer, Director
Submitted By:	Lee Ann Bunselmeyer, Director
City Manager Review:	**Approval:** Bob Hart, City Manager
Strategic Goals:	Citizen Engagement & Proactive Government

AGENDA ITEM

Receive a report, hold a discussion, and give staff direction on the Water and Wastewater Rates.

AGENDA ITEM SUMMARY/BACKGROUND

To maintain financial sustainability, the City performs a cost of service and rate design study for the City's water and wastewater utility on an annual basis. The study's intent is to achieve a water and wastewater structure that will assure equitable and adequate revenues for operations, debt service retirement, capital improvements and bond covenant requirements. Therefore, ensuring the utility operates on a self-sustaining basis while considering the economic impact on the City's customers. The analysis examined revenue requirements for a five-year period beginning with fiscal year 2020-2021.

Staff will provide an overview of the FY2020 water and wastewater rate analysis.

RECOMMENDATION

WORKSHOP BUSINESS ITEM 2.

City Council Regular and Workshop Session

Meeting Date: 02/20/2020

Title: Lake Cities Fire Department Overview

Submitted For: Bob Hart, City Manager **Submitted By:** Lee Ann Bunselmeyer, Director

City Manager Review: Bob Hart, City Manager

AGENDA ITEM

Receive a Presentation and hold a discussion regarding the Lake Cities Fire Department/Joint Lake Cities Council Meeting.

AGENDA ITEM SUMMARY/BACKGROUND

The Lake Cities Fire Department is a progressive organization that provides fire, rescue, and emergency medical services. The Department consists of a combination of 53 full-time firefighters, paramedics, and administrative personnel. The department currently operates out of three fire stations and a fire headquarters.

In 2016, the three cities (Hickory Creek, Lake Dallas, and Shady Shores) renewed a five-year inter-local agreement with the City of Corinth for Fire services. The **Fire** district is approximately 30 square miles with a combined population of approximately 35,000.

Staff will provide the City Council with a general overview of the Lake Cities Fire Department operations, structure, performance measures, staffing levels, and options that can position the department to best manage the community's anticipated funding requirements.

RECOMMENDATION

N/A

CONSENT ITEM 1.

City Council Regular and Workshop Session

Meeting Date:	02/20/2020		
Title:	Interlocal Agreement with Missouri City		
Submitted For:	Lee Ann Bunselmeyer, Director		
Submitted By:	Cindy Troyer, Purchasing Agent		
Finance Review:	Yes	**Legal Review:**	N/A
City Manager Review:	**Approval:** Bob Hart, City Manager		
Strategic Goals:	Regional Cooperation		

AGENDA ITEM

Consider and act on approval of an Interlocal Agreement with the City of Missouri City for cooperative purchasing.

AGENDA ITEM SUMMARY/BACKGROUND

Chapter 271, Subchapters D and F of the Local Government Code permit local government to enter into agreements with other public agencies in the interest of cooperatively sharing resources for their mutual benefit and take advantage of potential cost savings for various goods and services.

The City of Missouri City is interested in purchasing two (2) Harley Davidson police motorcycles from the City of Corinth. The motorcycles are no longer needed within the Police Department. The request to dispose of the two motorcycles was approved by the City Manager on February 6, 2020. The motorcycles are being sold at the wholesale book/clean trade value.

Missouri City is presenting the Interlocal Agreement to their City Council for approval on February 17, 2020.

RECOMMENDATION

Staff recommends approval of the Interlocal Agreement between the City of Corinth and the City of Missouri City.

Attachments

Interlocal Agreement

Bills of Sale

Interlocal Agreement between the City of Missouri City and the City of Corinth for the Purchase of Police Motorcycles

This Agreement is made and entered into pursuant to the Interlocal Cooperation Act, Chapter 791 of the Texas Government Code, by and between the CITY OF CORINTH, a municipal corporation of the State of Texas (hereinafter, "Corinth"), and the CITY OF MISSOURI CITY a municipal corporation of the State of Texas, acting herein by and through their City Council (hereinafter, "Missouri City").

WHEREAS, Chapter 791 of the Texas Government Code, as amended, provides authorization for units of local government to enter into interlocal cooperation agreements to perform governmental functions and services; and

WHEREAS, Corinth desires to transfer, sell, and convey and Missouri City desires to purchase and acquire certain police motorcycles; and

WHEREAS, the parties have determined that the transaction contemplated herein is in the best interest of their respective residents and promotes increased public safety; and

WHEREAS, such motorcycles are no longer required by Corinth and are desired by Missouri City in the performance of the governmental function of law enforcement;

NOW, THEREFORE, in consideration of the foregoing and further consideration of the mutual promises, covenants and conditions herein, Missouri City and Corinth hereby agree as follows:

Section 1. Purpose: The purpose of this Agreement between Missouri City and Corinth is to establish terms and conditions for the sale and transfer of two police motorcycles.

Section 2. Duties and Responsibilities of Corinth:

a. Corinth shall sell and transfer all right, title, and ownership in and to two (2) 2015 Harley-Davidson Electra Glide police motorcycles, described as follows:

1. VIN: 1HD1FMM19FB632018	License Plate: XY2071	Mileage: 7,188
2. VIN: 1HD1FMM12FB631972	License Plate: XY2072	Mileage: 6,715

(hereinafter, "Motorcycles").

b. Corinth shall execute or cause to be executed all necessary forms and instruments for the transfer of title to the Motorcycles, and any manufacturer's, dealer's, or other existing warranties, to Missouri City.

c. Corinth shall provide Missouri City reasonable access to the site on which the Motorcycles are stored to allow Missouri City to: (1) inspect the Motorcycles before the purchase of such Motorcycles; and (2) remove and transport such Motorcycles after the purchase thereof.

d. Prior to the purchase and transfer of the Motorcycles to Missouri City, Corinth shall provide Missouri City with any written vehicle history report or any report or log of service, maintenance, or repairs performed on each vehicle then existing, and Corinth shall disclose any known defect of each vehicle or any component, equipment, or accessory thereof, including but not limited to any head lamp; tail lamp; brake light; police light or siren; onboard radar, LIDAR, or any other speed-detecting device; or onboard computer or global positioning system (GPS) device.

Section 3. Duties and Responsibilities of Missouri City:

a. Missouri City shall pay Corinth upon thirty (30) days of receiving an invoice for the purchase of the Motorcycles the sum of nine thousand seven hundred dollars ($9,700.00) for each motorcycle for a total cost of nineteen thousand four hundred dollars ($19,400.00).

b. Missouri City shall, prior to the purchase and transfer of the Motorcycles to Missouri City, fully inspect the Motorcycles and fully make all investigations as it deems necessary and appropriate to ascertain the condition of the Motorcycles and the character and suitability thereof. Following the latter of such inspection or the receipt of information pursuant to subsection 2(d), above, Missouri City may terminate this Agreement immediately upon written notice to Corinth without penalty to either party.

Section 4. Administration: The City Manager or his designee for each respective party is authorized to act on behalf of such party in all matters relating to this Agreement.

Section 5. Insurance and Liability: Each party shall be responsible for its own negligent actions and the actions or omissions of its employees, officers, volunteers and agents, regardless of geographical location. Each party shall procure and maintain, at its sole and exclusive expense, insurance coverage, including comprehensive liability, personal injury, property damage, and workers compensation, with such limits of coverage and deductibles as are prudent and reasonable for the protection of itself, its personnel and its equipment. No party hereto shall have any obligation to provide or extend insurance coverage for any of the events, services, personnel or physical equipment of the other party required to provide services, as enumerated herein, to any other party or its personnel.

By this paragraph, neither party waives or relinquishes any immunity from liability, limitation of liability, or defense on behalf of itself, its officers, employees, volunteers and agents provided by the Constitution and laws of the state of Texas as a result of its execution of this Agreement and the performance of the covenants contained herein.

Responsibility for any damage due to vandalism, burglary, collision, or any other act committed by a third party or any natural disaster or occurrence, to the Motorcycles, shall be borne by the party in possession of the Motorcycles at the time such damage is incurred.

Section 6. No Partnership: It is agreed that nothing herein contained is intended nor should be construed as creating or establishing a relationship of co-partners or partnership between the

parties, or as creating or establishing the relationship by either party as agent, representative, or employee of the other party for any purpose, or in any manner, whatsoever.

Section 7. Severability: The provisions of this Agreement are severable. If any paragraph, section, subdivision, sentence, clause, or phrase of this Agreement is for any reason held to be invalid or contrary to the law by a court of competent jurisdiction or contrary to any rule or regulation in the remaining portions of the Agreement, it shall not affect, impair, or invalidate this Agreement as a whole or any provision hereof not declared to be invalid or contrary to law. However, upon the occurrence of such event, either party may terminate this Agreement forthwith upon the delivery of written notice of termination to the other party.

Section 8. Entire Agreement; Requirement of a Writing: It is understood and agreed that the entire Agreement of the parties is contained herein and that this Agreement supersedes all oral Agreements and negotiations between the parties relating to the subject matter hereof as well as any previous Agreement presently in effect between the parties relating to the subject matter hereof. Any alterations, amendments, deletions, or waivers of the provisions of this Agreement shall be valid only when expressed in writing and duly signed by the parties.

Section 9. Compliance with Laws and Regulations: It is understood that the terms and conditions of this Agreement are governed by the laws of the State of Texas.

Both parties shall abide by all statutes, ordinances, rules, and regulations pertaining to, or regulating the respective obligations of each party herein, including those now in effect and hereafter adopted. Any violation of said statutes, ordinances, rules or regulations shall constitute a material breach of this contract, and shall entitle either party to terminate this contract immediately upon delivery of written notice to the other party.

Section 10. Term: It is expressly understood and agreed that this Agreement shall take effect on the last date of execution hereof and shall continue until the parties have fully satisfied their obligations hereunder, unless terminated sooner by either party. Either party may terminate, with cause, immediately by providing written notice to the other party, or without cause, by giving at least thirty (30) days written notice to the other party.

Section 11. Notices:

a. Notice to Corinth shall be sent to:

City of Corinth
Attn: City Manager
3300 Corinth Parkway
Corinth, Texas 76208

b. Notice to Missouri City shall be sent to:

City of Missouri City
Attn: City Manager
1522 Texas Parkway
Missouri City, Texas 77489

With a copy to:

Missouri City Police Department
Attn: Chief of Police
3849 Cartwright Road
Missouri City, Texas 77459

Section 12. Current Revenues and Fair Compensation: Each party understands and agrees that each party paying for the performance of governmental functions or services under this Agreement must make those payments from current revenues available to the paying party. Missouri City's fiscal year is October 1 through September 30. If, for any reason, funds are not appropriated to continue the contract in the new fiscal year, said contract shall become null and void on the last day on which the funds are appropriated. The Agreement will then be terminated without penalty of any kind or form to Missouri City.

By entering into this Agreement, each party hereby declares that any payments furnished under this Agreement are in an amount that fairly compensates the performing party for the services or functions performed under the contract.

Section 13. Beneficiaries: This Agreement is solely for the benefit of Missouri City and Corinth and shall not be construed to confer any benefit on any other person or party except as expressly provided for herein.

Section 14. Choice of Law and Venue: This Agreement shall be governed by the laws of the State of Texas, except any conflict of law provisions, with venue in a court of competent jurisdiction in Fort Bend County, Texas. Corinth hereby consents to such jurisdiction and venue.

Section 15. Assignment: Neither party may assign any rights or obligations under this Agreement without the prior written consent of the other party to the Agreement.

EXECUTED this ___ day of _____, 20____.

CITY OF MISSOURI CITY

_____
Yolanda Ford Date
Mayor

CITY OF CORINTH

_____
Bob Hart Date
City Manager

ATTEST:

_____
Maria Jackson Date
City Secretary

_____
Kimberly Pence Date
City Secretary

Asset ID#2200-481

BILL OF SALE

STATE OF TEXAS

COUNTY OF DENTON

KNOW ALL MEN BY THESE PRESENTS that I, Bob Hart, City Manager for the City of Corinth, Texas, duly authorized seller, for and in consideration of the sum nine thousand seven hundred dollars ($9,700.00) to be paid by the City of Missouri City in the form of a check on this 21st day of February, 2020, and I being duly authorized by the City of Corinth, Texas, have sold and conveyed, and do hereby sell and convey unto the City of Missouri City the following described personal property:

2015 Harley Davidson VIN# 1HD1FMM19FB632018

Signed: _____

Printed Name:_____

Title: City Secretary

Subscribed and sworn to before me this the _____ day of _____ 20___.

_____

Notary Public in and for _____ County, TX.
My Commission Expires _____ 20____.
(If required)

Asset ID#2200-482

BILL OF SALE

STATE OF TEXAS

COUNTY OF DENTON

KNOW ALL MEN BY THESE PRESENTS that I, Bob Hart, City Manager for the City of Corinth, Texas, duly authorized seller, for and in consideration of the sum nine thousand seven hundred dollars ($9,700.00) to be paid by the City of Missouri City in the form of a check on this 21st day of February, 2020, and I being duly authorized by the City of Corinth, Texas, have sold and conveyed, and do hereby sell and convey unto the City of Missouri City the following described personal property:

2015 Harley Davidson VIN# 1HD1FMM12FB631972

Signed: _____

Printed Name:_____

Title: City Secretary

Subscribed and sworn to before me this the _____ day of _____ 20___.

_____

Notary Public in and for _____ County, TX.
My Commission Expires _____ 20____.
(If required)

CONSENT ITEM 2.

City Council Regular and Workshop Session

Meeting Date:	02/20/2020
Title:	Technology Services Security Policies
Submitted For:	Lee Ann Bunselmeyer, Director
Submitted By:	Shea Rodgers, Technology Services Manager
Finance Review:	N/A **Legal Review:** N/A
City Manager Review:	**Approval:** Bob Hart, City Manager
Strategic Goals:	Citizen Engagement & Proactive Government Organizational Development

AGENDA ITEM

Consider and act on a Resolution reviewing and approving the Technology Services Security Policy for the City of Corinth; and providing an effective date.

AGENDA ITEM SUMMARY/BACKGROUND

Per the recommendations of a cyber security assessment performed by The Fulcrum Group in 2019, Technology Services has created a Technology Security Policy. These documents outline some key actions and requirements necessary to maintain the security of the City's data, and what to do should that security be compromised.

The Technology Security Policy (attached: TECHNOLOGY SECURITY POLICY) is written to identify key weaknesses in cyber security and data privacy and the means by which to rectify those weaknesses. Among the subsections of the policy are guidelines for the following:

1. How Technology Services staff should treat data and its privacy.
2. How all City staff should treat sensitive data (credit card/banking, health, or criminal justice information).
3. The proper disposal methods of technology devices.
4. The understanding by City staff that their web browsing may be logged and access to certain sites may be restricted.
5. The procedures for outside vendors to access City resources for troubleshooting purposes.

RECOMMENDATION

Understanding that adopting and adhering to the Plan and Policies presented would provide a more secure data infrastructure, it is the recommendation of City staff that the City Council approve the Technology Services Security Policy effective February 21, 2020.

Attachments

RESOLUTION

TECHNOLOGY SECURITY POLICY

RESOLUTION NO._____

A RESOLUTION REVIEWING AND APPROVING THE TECHNOLOGY SERVICES SECURITY POLICY FOR THE CITY OF CORINTH; AND PROVIDING AN EFFECTIVE DATE.

WHEREAS, the City Council has reviewed and approved the Technology Services Security Policy attached hereto as Exhibit A, and

NOW, THEREFORE, THE COUNCIL OF THE CITY OF CORINTH HEREBY RESOLVES:

SECTION 1. That the City Council has reviewed the attached Technology Services Security Policy, which is designed to identify key weaknesses in cyber security and data privacy and the means by which to rectify those weaknesses.

SECTION 2. That all resolutions or parts of resolutions in force when the provisions of this resolution became effective which are inconsistent or in conflict with the terms or provisions contained in this resolution are hereby repealed to the extent of any such conflict only.

SECTION 3. That this resolution shall take effect immediately upon its passage and approval.

PASSED AND APPROVED this the 20th day of February 2020.

_____
Bill Heidemann, Mayor

ATTEST:

_____
Kim Pence, City Secretary

EXHIBIT A- TECHNOLOGY SERVICES SECURITY POLICY

CITY OF CORINTH

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE

SECTION:	TECHNOLOGY SERVICES	REFERENCE NUMBER:
SUBJECT:	POLICY	EFFECTIVE DATE 03/01/2020
TITLE:	TECHNOLOGY SECURITY POLICY	*LAST REVISION DATE:* 03/01/2020

1.0 PURPOSE

This Policy outlines the general practices and procedures to ensure the safety and security of the City of Corinth's network and IT infrastructure. By adopting certain practices and procedures, the City may significantly reduce its overall IT risk and mitigate the effects of an Adverse Computer Event.

This Policy will provide guidelines and expectations for the Technology Services (TS) Department, City Staff, and external Third-Parties and vendors, and dictate potential disciplinary actions and repercussions for non-compliance. The provisions of this Policy do no supersede any local, state, or federal laws, nor any other City policies regarding confidentiality, information dissemination, or standards of conduct.

2.0 DEFINITIONS

2.1 Adverse Computer Event – An event with a negative consequence to an information systems network, such as: unauthorized use of system privileges, unauthorized access to Sensitive Information/Data, or execution of malware that destroys data or holds it for ransom.

2.2 Authorized User – Any Staff Member that has been approved to have access to a particular system owned by the City.

2.3 City – City of Corinth, Texas.

2.4 City Council – The elected legislative body of the City of Corinth, Texas.

2.5 City Manager – The person appointed as the City Manager of the City of Corinth, Texas.

2.6 Director – An employee designated by the City Manager as a director-level position.

2.7 Encrypted Data – Any file, database, or information that has undergone Encryption.

2.8 Encryption – A process by which data is safeguarded by encoding it so that only the authorized parties can access it.

2.9 End-User – Any part-time or full-time employee, contract employee, temporary employee, City Council member, or volunteer with access to Information Systems at the City.

2.10 Information System – Any technology system that stores, accesses, or maintains data owned by the City.

2.11 Personal Identifiable Information (PII) – Any data that could potentially identify a specific individual (e.g., Social Security Numbers, Driver's License Numbers, etc.). Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered.

2.12 Proprietary Information – Information that could reasonably be expected to be guarded from public knowledge. This could include information about Staff Members, the public, or other information about official City business that is not subject to Open Records.

2.13 Protected Health Information (PHI) – Under US law, any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

2.14 Sensitive Information/Data – Information or data, Encrypted or not, whose content requires that the security and integrity of the data are not compromised. This Data must be protected against unauthorized access. It may contain PII, PHI, financial data (such as credit card information or bank account numbers), or other Proprietary Information.

2.15 Staff Member – Any part-time or full-time employee, contract employee, temporary employee, City Council member, or volunteer doing business in an official capacity on behalf of the City.

2.16 Technology Services Department – The department assigned by the City Manager to administer the City's technological services and property.

2.17 Third-Party – An outside firm or individual with whom the City is contracting for services.

3.0 PROCEDURES

3.1 TECHNOLOGY SERVICES NON-DISCLOSURE AGREEMENT

3.1.1 Preface/Purpose – To perform their job duties in support of the City of Corinth's mission, employees in TS support roles are frequently provided privileged access to the Information Systems that they support and to the data and records managed by those systems. Privileged access imposes upon the TS employee the responsibility and obligation to use that access in an ethical, professional, and legal manner that is strictly within his or her job function.

The City is committed to advancing the ethical and responsible use of all information resources and does not tolerate illegal, dishonest, improper, or irresponsible use.

3.1.2 In exchange for the elevated access privileges afforded to the TS employee, he or she agrees to abide by the following performance standards:

3.1.2.1 Take every reasonable precaution to prevent unnecessary or unauthorized access to any passwords, user identification, or other information that may be used to access Information Systems, whether the data contained therein belong to the City or private parties.

3.1.2.2 Limit access to the information contained in or obtained from Information Systems to authorized persons.

3.1.2.3 Treat all information encountered in the performance of any job function as confidential unless advised otherwise by a supervisor.

3.1.2.4 Seek guidance from a supervisor whenever the TS employee is unsure of the correct decision regarding the appropriate use and confidentiality of information, and to do so before the TS employee takes any action that might compromise that use or confidentiality.

3.1.2.5 Upon the request by a Staff Member for access to information, the TS employee must obtain in writing the approval of the Director (or designee) of the department acting as the data owner (e.g., Director of Human Resources for disciplinary information, or Director of Finance for financial information).

3.1.2.6 Avoid any sharing, recording, transmission, alteration, or deletion of information in the Information Systems except as required in the performance of the TS employee's job duties.

3.1.2.7 Avoid accessing or reading data in any Information System that is not immediately required by the TS employee's job duties.

3.1.2.8 Strictly comply with all City policies related to the use and security of City Information Systems or resources.

3.1.2.9 Report any incidents of non-compliance with the terms of this Policy to a supervisor.

3.1.3 Scope – This policy applies to all Technology Services employees, and to all Information Systems under the administration of the Technology Services Department, regardless of the ownership of the device or data.

3.2 **SECURE DATA PROCEDURES**

3.2.1 Preface/Purpose – To provide guidance and regulations for the security of data held on City Information Systems, servers, or workstations, including the transmission of data on the City's network, this section outlines the requirements of the proper handling of this data.

The section of this Policy is not intended to supersede any local, state, or federal laws. Rather it is designed to reinforce the policies and procedures as outlined in the appropriate framework (e.g., PCI for financial data, HIPAA for medical data, CJIS for criminal justice data).

3.2.2 Staff Members, contractors, Third-Parties, vendors, and agents operating with City data or Information Systems, or acting in an official capacity for the City while using servers, workstations, or the City's network shall consider the sensitivity of the respective information, including cardholder data, Personally Identifiable Information (PII), Protected Health Information (PHI), et al. in order to minimize the possibility of unauthorized access.

3.2.3 Physical and electronic documentation containing Sensitive Data shall be stored in a secure method as outlined in the respective data's frameworks, and shall be destroyed in accordance with local and state law when no longer needed.

3.2.4 Destruction of information may include paper shredding, paper burning, hard drive shredding/physical destruction, magnetic hard drive degaussing, or Department of Defense (DOD)-compliant software destruction. These destruction methods may be performed by City Staff or by an outside firm with verification that one of these methods is performed (see Section 3.3 "TECHNOLOGY DISPOSAL").

3.2.5 City Staff will implement and follow physical and technical safeguards for all workstations that transmit, store, or process Sensitive Data in order to limit access to authorized City Staff or Third-Parties and for official use only.

3.2.6 Appropriate measures to ensure physical and technical security include, but are not limited to:

3.2.6.1 Restrict physical access to workstations, servers, or the City network to only authorized City Staff or Third-Parties.

3.2.6.2 Secure workstations or servers by locking the screen or logging out prior to leaving the area, even temporarily.

3.2.6.3 Enable a password-protected screen saver with a timeout period no longer than fifteen (15) minutes. Passwords must comply with the City's guidelines and regulation on password complexity.

3.2.6.4 Ensure that workstations, particularly those used to transmit Sensitive Data, are used for official City business use only.

3.2.6.5 Never install unauthorized software on City Information Systems. All software must be approved by a member of the TS staff prior to installation, regardless of whether or not the software requires administrative credentials to install

3.2.6.6 Storing Sensitive Data on TS supported network servers or TS approved cloud-based solutions, and only when required by the respective data framework.

3.2.6.7 Secure laptops or mobile devices that contain Sensitive Information with Encryption, and ensure their physical security by using cable locks or locking the offices/rooms in which they are stored.

3.2.6.8 Install privacy screen filters or use other physical barriers to help prevent the unwanted exposure of data.

3.2.6.9 Ensure that workstations are locked or users are logged out, but left powered-on to facilitate after-hours updates.

3.2.7 Scope – This section applies to all City Staff Members or Third-Parties operating Information Systems that store or transmit Sensitive Information.

3.3 **TECHNOLOGY DISPOSAL**

3.3.1 Preface/Purpose – In order to ensure the protection of Sensitive Data, the section of this Policy outlines the specific measures Staff Members must take when disposing of technology devices. This section is not intended to supersede any local, state, or federal laws or policies, but to provide regulations beyond simple disposal of devices.

3.3.2 When technology assets have reached the end of their useful life, they shall be sent to the Technology Services Department for proper disposal.

3.3.3 Technology Services shall ensure the complete destruction of the data on the device by hard drive shredding/physical destruction, magnetic hard drive degaussing, or Department of Defense (DOD)-compliant software destruction. The latter must overwrite each and every sector of the hard drive/storage medium no fewer than seven (7) times. This process may be completed by TS Staff Members or by a Third-Party who can verify the destruction of the data.

3.3.4 Once the data/storage medium has been destroyed, or should TS employees determine that no data is stored on the device, normal surplus, auction, and disposal means may be undertaken as outlined in the Purchasing Policy.

3.3.5 Due to the nature of the chemicals and elements in technology devices, no computer equipment shall be disposed of in landfills or dumps. If not auctioned off, they should be recycled or given to a Third-Party to dispose of properly.

3.3.6 No computer or technology asset may be sold, donated, or disposed of through any means other than this Policy and the Purchasing Policy.

3.3.7 Scope – This section applies to all technology devices, including but not limited to: computers, laptops, tablets, cell phones, servers, computer components, printers, monitors, backup tapes, and networking devices.

3.4 **EMPLOYEE INTERNET MONITORING/FILTERING**

3.4.1 Preface/Purpose – In order to ensure the safety of the City's network and to comply with local, state, and federal laws and policies, this section of the Policy outlines steps Technology Services may take to monitor and filter internet and web browsing traffic.

3.4.2 The Technology Services Department may install, configure, and maintain hardware or software that monitors all traffic on the City's networks (wired, wi-fi, and cellular networks).

3.4.2.1 The information collected by this hardware or software may include, but is not limited to: employee names, employee usernames, time accessed, website visited, duration of visit, source and destination IP addresses, computer names, protocols, and ports.

3.4.2.2 The information may be kept for up to 180 days.

3.4.2.3 No Personal Identifiable Information (PII), such as passwords, identification numbers, etc., will be collected or retained.

3.4.2.4 Without the Staff Member's knowledge or consent, the Technology Services Department may compile a report of Staff Members' internet browsing history in order to determine trends, comply with a Director's request, cooperate with a criminal investigation, or respond to an Adverse Computer Event.

3.4.2.5 Reports of browsing history may be made available to the City Manager, Human Resources Director, to the Staff Member's department Director upon request.

Note that these reports are subject to the Texas Public Information Act.

3.4.3 The Technology Services Department shall install, configure, and maintain hardware or software to filter the web browsing traffic on the City's networks (wired, wi-fi, and cellular networks).

3.4.3.1 Examples of categories of sites that may be blocked include but are not limited to: adult/sexually explicit material, chat and instant messaging, gambling, hacking, illegal drugs, intimate apparel and swimwear, peer-to-peer file sharing, personals and dating, spam/phishing/fraud, spyware, tasteless and offensive content, violence, intolerance, and hate.

3.4.3.2 The Technology Services Department may at any time modify the list of blocked websites/categories at the direction of the City Manager or Technology Services manager. These changes may or may not be communicated to Staff Members.

3.4.3.3 At the request of the City Manager, Technology Services manager, or Department Director, and with a valid business purpose, TS may create exceptions to the website filtering policy. These exceptions may correct miscategorized websites, allow a particular website to an individual or group, or allow an individual or group to browse unrestricted.

Note that browsing history shall still be recorded regardless of any exceptions made to website filtering policies.

3.4.4 Scope – This section applies to all Staff Members using a computer, laptop, cell phone, or tablet owned by the City, or operating a device regardless of ownership on a network owned and operated by the City.

3.5 **VENDOR/THIRD-PARTY ACCESS**

3.5.1 Preface/Purpose – In order to better support Third-Party applications, the Technology Services Department may periodically allow access to City-owned systems, servers, and network to various vendors and Third-Parties. This section of this Policy outlines requirements to maintain the security of the City's technology infrastructure.

3.5.2 No vendors or Third-Parties may have access to any City-owned system, workstation, server, or network device without first being invited by an Authorized User.

3.5.3 For remote sessions, the application by which the Third-Party connects to the City resource must be configurable in such a way that only those being invited can connect, achievable by *two or more* of the following:

3.5.3.1 Utilizing application passwords (e.g., a password on the TeamViewer application that is required to connect)

3.5.3.2 Static originating IP addresses that can be whitelisted in a firewall

3.5.3.3 Consistent protocols and ports that can be whitelisted in a firewall

3.5.3.4 Opening a secured VPN tunnel controlled by the City of Corinth

3.5.3.5 An assumption of liability agreement signed by the City and Third-Party to the satisfaction of the City of Corinth Legal department

3.5.4 Once representatives from the Third-Party have accessed the City resource, either physically in-person or remotely, the Authorized User must remain present and attentive to the actions being taken until the Third-Party representatives have physically left or closed the remote session.

3.5.5 Should the Authorized User observe the Third-Party taking action that could undermine security, he or she must stop the access for the Third-Party and notify Technology Services immediately.

3.5.6 All changes the Third-Party makes on the service, system, or network device must be reviewed and approved by TS staff to ensure information security is maintained.

3.5.7 Under no circumstances are vendors/Third-Parties to change network firewalls or alter any other security protocol without the expressed prior consent of TS staff.

3.5.8 No City-owned data is to move off-site without the expressed consent of TS staff, who will monitor and administer all data exfiltration.

3.5.9 All software and hardware maintenance contracts with vendors or Third-Parties must be approved by the Technology Services manager (or designee) prior to the execution of the contract.

3.5.10 The TS department may, for any reason, terminate the remote connection from Third-Parties, or remove their physical access, and may revoke any future access for any violations of this Policy.

3.5.11 Scope – This section applies to all technology devices, including but not limited to: computers, laptops, tablets, cell phones, servers, and networking devices, and to any vendor or Third-Party operating in support of hardware or software the City has purchased.

4.0 VIOLATIONS

4.1 Any Staff Member who knowingly violates any of these terms, or facilitates the violation of these terms by others, is subject to disciplinary action, up to and including termination.

4.2 Any Staff Member who observes or is made aware of actions taken contrary to this Policy, and does not immediately notify Technology Services staff is subject to disciplinary action, up to and including termination.

4.3 Should a Staff Member's action incidentally contribute to an Adverse Computer Event or the potential for reduced security, or otherwise act contrary to this Policy, that Staff Member is subject to disciplinary action, up to and including termination.

4.4 All Adverse Computer Events or potential events shall be investigated by Technology Services staff, who will act according to the Incident Response Plan.

4.5 Any Third-Party or vendor not operating in accordance with this Policy shall have their access revoked. The decision to restore access to City-owned infrastructure will be made on a case-by-case basis by the Technology Services Manager

CONSENT ITEM 3.

City Council Regular and Workshop Session

Meeting Date:	02/20/2020
Title:	Utility Bill Processing and Printing
Submitted For:	Lee Ann Bunselmeyer, Director
Submitted By:	Chris Rodriguez, Financial Services Manager
Finance Review:	Yes **Legal Review:** N/A
City Manager Review:	**Approval:** Bob Hart, City Manager
Strategic Goals:	Citizen Engagement & Proactive Government Regional Cooperation

AGENDA ITEM

Consider approval of the DataProse contract renewal and expenditures for bill processing, postage and inserts.

AGENDA ITEM SUMMARY/BACKGROUND

The DataProse contract for utility bill processing and mailing is up for renewal this month. Staff would like to renew the contract for another year by piggy backing on Plano's contract with DataProse. This would be our second year to piggy back on Plano's contract with DataProse. The annual contract for bill processing is $15,606, postage to mail the bills is estimated at $41,000, and the cost for inserts is approximately $9,000 for a total estimated annual cost of $65,606. The postage is included in our cost because DataProse mails the bills once they are processed.

RECOMMENDATION

Staff recommends approval of the one-year renewal with DataProse for utility bill processing and mailing.

Attachments

DataProse Renewal Letter

DATAprose®

February 12, 2020

Bob Hart
City Manager
City of Corinth
3300 Corinth Parkway
Corinth, TX 76208

Re: Contract Renewal

Thank you for putting your trust in DataProse and allowing us to handle your billing processing and printing production process. This letter serves as notice of our intent to renew the contract with the City of Corinth. The contract renewal will begin on February 22, 2020 and will continue for a period of not less than one (1) year, ending on February 22, 2021. This contract renewal supersedes all prior agreements and replaces all written agreements between both parties hereto relating to the subject matter hereof.

As busy as you and I are, it's virtually impossible to stay informed of every issue, every day. So I urge you to let me know when we are hitting or missing the mark. We strive to be the best and we thrive on client feedback. My direct phone number is (972) 462-5410.

By both parties signing our signature below, signifies that we are both in agreement with this extension to your contract.

IN WITNESS WHEREOF, The parties hereto have caused this Agreement to be executed to be effective as of the Effective Date.

DATAPROSE Curtis Nelson

Chief Operation Officer

Date: 02/12/2020

CLIENT **City of Corinth**

City Manager

Date:

Once again, thank you very much for your continued trust. I look forward to hearing from you.

Sincerely,

Curtis Nelson
Chief Operating Officer, DataProse, LLC

CONSENT ITEM 4.

City Council Regular and Workshop Session

Meeting Date:	02/20/2020
Title:	Incident Response Plan
Submitted For:	Lee Ann Bunselmeyer, Director
Submitted By:	Lee Ann Bunselmeyer, Director
Finance Review:	N/A **Legal Review:** N/A
City Manager Review:	**Approval:** Bob Hart, City Manager
Strategic Goals:	Citizen Engagement & Proactive Government Organizational Development

AGENDA ITEM

Consider and act on a Resolution reviewing and approving the Incident Response Policy and Plan for the City of Corinth and Providing an Effective Date.

AGENDA ITEM SUMMARY/BACKGROUND

Per the recommendations of a cyber security assessment performed by The Fulcrum Group in 2019, Technology Services has created an Incident Response Plan (IRP). These documents outline some key actions and requirements necessary to maintain the security of the City's data, and what to do should that security be compromised.

The Incident Response Plan (attached: TECHNOLOGY SERVICES IRP - PLAN) and associated policy to adopt that IRP (attached: TECHNOLOGY SERVICES IRP - POLICY) identify key members of City staff that would be members of an Incident Responst Team (IRT). The IRT is activated when a data breach or adverse computer event has occured, with each member of the IRT having specific tasks and roles as outlined in the IRP. At the conclusion of the incident, City staff would complete a report (attached: TECHNOLOGY SERVICES IRP - REPORT) that would log the events. The IRP is designed to reduce prolonged risk to the City's infrastructure and mitigate the effects of an incident that compromises cyber security.

RECOMMENDATION

Understanding that adopting and adhering to the Plan and Policies presented would provide a more secure data infrastructure, it is the recommendation of City staff that the City Council approve the Technology Services Incident Response Plan effective February 21, 2020.

Attachments

RESOLUTION
TECHNOLOGY SERVICES IRP - PLAN
TECHNOLOGY SERVICES IRP - POLICY
TECHNOLOGY SERVICES IRP - REPORT

RESOLUTION NO._____

A RESOLUTION REVIEWING AND APPROVING THE INCIDENT RESPONSE POLICY AND PLAN FOR THE CITY OF CORINTH; AND PROVIDING AN EFFECTIVE DATE.

WHEREAS, the City Council has reviewed and approved the Incident Response Policy and Plan attached hereto as Exhibit A, and

NOW, THEREFORE, THE COUNCIL OF THE CITY OF CORINTH HEREBY RESOLVES:

SECTION 1. That the City Council has reviewed the attached Incident Response Policy and Plan, which is designed to reduce prolonged risk to the City's infrastructure and mitigate the effects of an incident that compromises cyber security.

SECTION 2. That the Director of Finance, Communication and Strategic Services is the chair of the Incident Response Team and is responsible for confirmation that an Adverse Computer Event or Breach involving Sensitive Information has occurred, notify the City Manager and Director of Human Resource and to coordinate the activities of the Incident Response Team .

SECTION 3. That all resolutions or parts of resolutions in force when the provisions of this resolution became effective which are inconsistent or in conflict with the terms or provisions contained in this resolution are hereby repealed to the extent of any such conflict only.

SECTION 4. That this resolution shall take effect immediately upon its passage and approval.

PASSED AND APPROVED this the 20th day of February 2020.

_____
Bill Heidemann, Mayor

ATTEST:

_____
Kim Pence, City Secretary

EXHIBIT A- INCIDENT RESPONSE POLICY AND PLAN

CORINTH
TEXAS

Computer & Sensitive Information Incident Response Plan

Effective: March 1, 2020

I. Incident Response Plan

An Incident Response Plan (IRP, Plan) is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or Incident at a Third-Party is traced back to the organization. The Plan identifies and describes the roles and responsibilities of the **Incident Response Team**, who is responsible for putting the plan into action.

II. Incident Response Team

An Incident Response Team (IRT, Team) is established to provide a quick, effective, and orderly response to computer-related Incidents such as virus infections, hacker attempts and break-ins, improper disclosure of Sensitive Information to others, system service interruptions, Breach of personal information, and other adverse events with serious information security implications. The IRT's mission is to prevent a serious loss of public confidence or information assets by providing an immediate, effective, and skillful response to any unexpected event involving computer information systems, networks or databases.

The IRT is authorized to take appropriate steps deemed necessary to contain, mitigate, or resolve an Adverse Computer Event. The Team is responsible for investigating suspected intrusion attempts or other security Incidents in a timely, cost-effective manner and reporting such findings to City Management, City Council, and the appropriate authorities as necessary.

The IRT will ensure that Technology Services personnel subscribe to various security industry alert services to keep abreast of relevant threats, vulnerabilities or alerts from actual Incidents.

A. Incident Response Team Members

The Incident Response Team will include:

- City Manager
- Director of Finance, Communications, and Strategic Services
- Technology Services Manager
- Director of Human Resources

Additional members of the IRT may include:

- City Attorney
- Any other member of the City staff, as designated by the City Manager

In the case of any Team member being absent, that member may appoint a designee from their Department to serve in their stead, with approval by the City Manager or Acting City Manager.

B. Incident Response Team Roles and Responsibilities

1. City Manager
   - Acts as a liaison between IRT and City Council members
   - Provides executive authority and decision making as needed during the Incident

2. Director of Finance, Communications, and Strategic Services
   - Manages and coordinates IRT actions in response to an Incident
   - Contacts members of the IRT
   - Determines which IRT members are required for the Incident
   - Escalates issues to City Manager as appropriate

3. Technology Services Manager
   - Determines the nature and scope of the Incident
   - Contacts qualified information security specialists for advice as needed
   - Provides proper training on Incident handling
   - Ensures evidence gathering, chain of custody, and preservation is appropriate
   - Prepares a written summary of the Incident and corrective action taken
   - Acts as a central Point of Contact (POC) for all computer Incidents
   - Notifies the Director of Finance, Communications, and Strategic Services to activate the Incident Response Team

4. Director of Human Resources
   - Documents the types of Sensitive Information that may have been Breached
   - Provides guidance throughout the investigation on issues relating to confidentiality of Sensitive Information
   - Assists in developing appropriate communication to impacted parties
   - Assesses the need to change privacy policies, procedures, and/or practices as a result of the Incident

5. Technology Services
   a. Assistant Technology Services Manager and Technology Services Specialists
      - Monitors business applications and services for signs of attack
      - Reviews audit logs of mission-critical servers for signs of suspicious activity
      - Contacts the IRT with any information relating to a suspected Incident
      - Collects pertinent information regarding the Incident at the request of the IRT
      - Reviews systems to ensure compliance with information security policy and controls
      - Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches
      - Reports any system control gaps to management for corrective action
      - Ensures backups are in place for all critical systems

b. Network Administrator
   - Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
   - Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers
   - Looks for signs of a firewall Breach
   - Contacts external Internet Service Providers for assistance in handling the Incident
   - Takes action necessary to block traffic from suspected intruder(s)
   - Examines system logs of critical systems for unusual activity

6. Communications Department
   - Designates a Communications and Marketing Coordinator to serve as a Public Information Officer (PIO)
   - Works with the City Manager to formulate a public response to the Incident, if deemed necessary by the City Manager

C. Incident Response Team Notification

Technology Services will be the central POC for reporting Adverse Computer Events and Breaches of Sensitive Information. Technology Services personnel will notify the Technology Services Manager in the case of any Adverse Computer Events. A preliminary analysis of the Incident will take place by the Technology Services Manager, who will coordinate with the Director of Finance, Communications, and Strategic Services to determine whether IRT activation is appropriate.

III. Types of Incidents

There are many types of Incidents that may require Incident Response Team activation. Some examples include:

- Breach of Sensitive Information
- Denial of Service / Distributed Denial of Service
- Excessive Port Scans
- Firewall Breach
- Computer Virus Outbreak

Breach of Sensitive Information - Overview

This IRP outlines steps the organization will take upon discovery of unauthorized access to Sensitive Information (i.e., Personal Identifiable Information (PII), Personal Health Information (PHI), Proprietary Information, etc.) that could result in harm or inconvenience to an individual or the City of Corinth operations.

In addition to the internal notification and reporting procedures outlined below, credit card companies require City officials to immediately report a security Breach, and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Specific steps are outlined in Appendix A. Selected laws and regulations require the organization to

follow specified procedures in the event of a Breach of personal information as covered in Appendix B.

Sensitive Information is information that is, or can be, about or related to an identifiable individual, or proprietary information related to City operations. It includes any information that can be linked to an individual or the City of Corinth, and used to identify an individual, or disclose confidential City operations information.

For our purposes, PII or PHI is defined as an individual's first name or first initial and last name, in combination with any of the following data:

- Social Security Number
- Driver's license number or Identification Card number
- Employee number
- Financial account numbers: credit or debit card number, bank account numbers, etc.
- Medical or health information

Proprietary Information relating to City operations is Sensitive Information that can disrupt or expose to harm the operations in support of the City, for example:

- Login name and passwords for computer systems
- Confidential City financial information
- Security information relating to the information systems network
- Response Plan documents

IV. Definition of an Adverse Computer Event

An Adverse Computer Event is an event with a negative consequence to an information systems network, such as: unauthorized use of system privileges, unauthorized access to Sensitive Information/data, or execution of malware that destroys data or holds it for ransom. Good-faith acquisition of Sensitive Information by an employee or agent of the City for business purposes is not an Adverse Computer Event.

V. Requirements/Responsibilities

All Authorized Users who access or utilize Sensitive Information should be identified and documented. Documentation must contain employee name, username, department, and level of access. This documentation will be kept in the employee's file in the Human Resources Department.

A. Authorized Users Responsibilities

Authorized Users that work with Sensitive Information play an active role in the discovery and reporting of any Adverse Computer Event or Breach. In addition, they can serve as a liaison between Technology Services and any Third-Party involved with a privacy Breach affecting the organization's data.

All City employees have an obligation to report any suspected or confirmed Adverse Computer Events or Sensitive Information Breach to Technology Services immediately upon discovery, regardless of their level of involvement in the event. That is to say, even if an

employee simply overhears something about an Incident, he or she is obligated to report it to a member of the IRT. This includes notification received from any Third-Party service providers or other business partners with whom the organization shares Sensitive Information. The Technology Services Manager will notify the Director of Finance, Communications, and Strategic Services, and other Department Directors and Managers whenever a suspected Breach of Sensitive Information affects their business area.

> Note: For ease of reporting, and to ensure a timely response 24 hours a day, seven days a week, an on-call designee of Technology Services will act as a central POC for reaching the Technology Services Manager. This designee can be reached by calling the Technology Services Helpdesk at:
> **(940) 498-3205, option 3**.

The Technology Services Manager will determine whether the potential Adverse Computer Event or suspected Sensitive Information Breach is serious enough to require the notification of the Director of Finance, Communications, and Strategic Services, in which case, the two departments will then determine if the event warrants a full IRT activation (see "Incident Response Team" section.) The reporting Authorized User may be tasked with assisting in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the IRT.

B. Department Directors and Managers Responsibilities

Department Directors and Managers are responsible for ensuring all employees in their unit are aware of policies and procedures for protecting Sensitive Information, and to prevent unauthorized access.

If an Adverse Computer Event or Sensitive Information Breach occurs in their Department, the Department Director or Manager must ensure Technology Services is notified immediately and a Track-It ticket is opened.

C. When Notification is Required

The following Incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or Third-Party provider) has obtained unauthorized access to Sensitive Information maintained in either paper or electronic form.
- An intruder has broken into database(s) that contain Sensitive Information.
- Computer equipment such as a workstation, laptop, CD-ROM, flash drive, or other electronic medium containing Sensitive Information has been lost or stolen.
- A department or unit has not properly disposed of media containing Sensitive Information.
- A Third-Party service provider has experienced any of the Incidents above, affecting the City's data containing Sensitive Information.

The following Incidents may not require notification under contractual commitments or applicable laws and regulations providing the City can reasonably conclude after investigation that misuse of the information is unlikely to occur:

- The City, Department, or Third-Party (Organization) is able to retrieve the Sensitive Information that was stolen, and based on a thorough investigation, reasonably concludes that retrieval took place before the Sensitive Information was copied, misused, or transferred to another person.
- The Organization determines that Sensitive Information was improperly disposed of but can establish that the Sensitive Information was not retrieved or used before it was properly destroyed.
- An intruder accessed files that did not contain Sensitive Information.
- A mobile device is lost or stolen, but the data is Encrypted and secure, or was deleted via mobile device management.

D. Incident Response – Adverse Computer Event

IRT members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

Technology Services Department

Contacts	Phone	E-Mail
Primary: Helpdesk	(940) 498-3205	TechnologyServices@cityofcorinth.com

1. Technology Services will serve as the central point of contact for reporting any suspected or confirmed Adverse Computer Event.

2. After documenting the facts presented by the caller and verifying that an Adverse Computer Event occurred, Technology Services will open an Adverse Computer Event Report and notify the Technology Services Manager.

Technology Services Manager (TSM)

Contact	Phone	E-Mail
Primary: Shea Rodgers	(940) 498-3250	Shea.Rodgers@cityofcorinth.com
Alternate contact info:	(940) 230-1515	

1. When notified, the TSM performs a preliminary analysis of the facts and assess the situation to determine the nature and scope of the Incident.

2. Identifies the systems and type(s) of information affected and determines whether the Incident could be an Adverse Computer Event, or suspected Breach of Sensitive Information. Every Incident may not require participation of all Incident Response Team members

3. Informs the Director of Finance, Communications & Strategic Services that a possible Incident has been reported and provides them an overview of the situation.

4. If an Adverse Computer Event or a Breach affecting Sensitive Information is confirmed, Incident Response Team activation is warranted.

5. Contact all Technology Services personnel to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the Incident.

6. Contact appropriate Incident Response Team members.

7. Work with the appropriate parties to determine the extent of the Incident. Identify any Sensitive Information/data stored and compromised on all test, development, and production systems.

Director of Finance, Communications, & Strategic Services (DFCSS)

Contact	Phone	E-Mail
Primary: Lee Ann Bunselmeyer	(940) 498-3241	LeeAnn.Bunselmeyer@cityofcorinth.com
Alternate contact info:	(940) 882-1668 (940) 882-2521	

1. After confirmation that an Adverse Computer Event or Breach involving Sensitive Information has occurred, notify the City Manager and Director of Human Resources.

2. Coordinate activities of the Computer and Sensitive Information Incident Response Plan.

3. Notify the City Attorney as appropriate. Provide a summary of confirmed findings, and of the steps taken to mitigate the situation.

4. Identify and contact the Director or Manager for the Department affected by the Incident. In coordination with the City Attorney, City Manager, and the Director of Human Resources, determine any legal or contractual notification requirements.

5. If the Incident occurred as a result of a Third-Party action or neglect, determine if a legal contract exists. Work with the City Attorney and City Manager to review contract terms and determine next course of action.

6. If an internal user (authorized or unauthorized employee, contractor, consultant, etc.) was responsible for the Incident, contact the Human Resources Director for disciplinary action and possible termination. In the case of contractors, temporary employees, or other Third-Party personnel, ensure discontinuance of the user's service agreement with the company.

7. Prepare appropriate response to media, community, City Council, and/or employees; send the response to the City Manager for approval or escalation to the City Council, if warranted.

8. Proactively respond to media inquiries, as necessary.

9. Monitor media coverage and circulate accordingly.

10. Vehicles for communicating include:

- News wire services
- Website
- E-mail
- News conference – If the Adverse Computer Event should reach a crisis level, coordinate a brief news conference at an appropriate location.

    - Appoint appropriate spokesperson
    - Prepare statement and, if necessary, potential Q & A.
    - Coach spokesperson on statement and potential Q & A.
    - Invite select media to attend and cover organization's proactive message.
    - Use the conference as a platform for communicating what the Incident involves, what the organization is doing to correct the Incident, how it happened, and the City's reassurance to the community.

City Manager (CM)

Contact	Phone	E-Mail
Primary: Bob Hart	(940) 498-3240	Bob.Hart@cityofcorinth.com
Alternate contact info:	(940) 783-0419 (940) 641-5042	

1. Review response crafted by the DFCSS. If warranted, escalate the response to the City Council for approval. If the situation is determined by the CM to not need escalation to the City Council, the CM may approve the response directly.

2. If necessary, notify the appropriate authorities (e.g., Police, FTC, FBI, TML, etc.).

3. Coordinate with the City Attorney and the Director of Human Resources on the timing, content and method of notification. If warranted, review, edit, approve, and issue the statement crafted by the DFCSS.

Director of Human Resources (DHR)

Contact	Phone	E-Mail
Primary: Guadalupe Ruiz	(940) 498-3230	Guadalupe.Ruiz@cityofcorinth.com
Alternate contact info:	(940) 882-1669	

1. Monitor relevant privacy-related legislation, provide input as appropriate, and communicate to employees the effect that any enacted legislation may have on them.

2. Be cognizant of major contracts which the City enters that may have an impact or effect on employees.

3. Be aware of other organizations' privacy policies that may affect the City and its affiliates.

4. Coordinate with other members of the IRT on the timing and content of any notifications to employees.

5. If the IRT determines that the Incident warrants law enforcement involvement, any notification to employees may be delayed if law enforcement determines the notification will impede a criminal investigation. Notification will take place after law enforcement determines that it will not compromise the investigation.

6. Follow any approved procedures for any notice to employees of unauthorized access to Sensitive Information.

4. Notifications to employees should be timely, conspicuous, and delivered in a manner that will ensure the notification is properly received. Notifications should be consistent with federal and state law, and any applicable city policies.

   Appropriate delivery methods may include:

   - Face-to-face spoken communication
   - Written notice
   - Email notice

   Information that may be considered to include in a notification to employees:

   - A general description of the Incident and what is being done to mitigate any further threat.
   - Remind employees to remain vigilant and to immediately report any potential Adverse Computer Events to Technology Services.
   - What to expect as far as City operational capability at present and what work will need to be done to return operations back to normal.
   - What the employees' response should be to questions directed to them by the media or public.

City Attorney

Contact	Phone	E-Mail
Primary: Messer, Fort, McDonald Law Firm Alternate contact info:	(972) 668-6400	

1. Monitor relevant privacy-related legislation, provide input as appropriate.

2. Be cognizant of major contracts which the City enters that may have an impact or effect on our customers, employees, and other data.

3. Be aware of other companies' privacy policies that may affect the city and its affiliates.

4. Coordinate with other members of the IRT on the timing and content of any notification to individuals.

5. If the IRT determines that the Incident warrants law enforcement involvement, any notification to individuals may be delayed if law enforcement determines the notification will impede a criminal investigation. Notification will take place after law enforcement determines that it will not compromise the investigation.

6. Follow approved procedures for any notification of unauthorized access to City-owned Sensitive Information.

7. Notification to individuals should be timely, conspicuous, and delivered in a manner that will ensure that the individual receives it. Notice should be consistent with Federal and State laws and City policies.

   Appropriate delivery methods include:

   - Written notice
   - Email notice
   - Substitute notice
     - Conspicuous posting of the notice on the website
     - Notification to major media

   Items to consider including in notification to individuals:

   - A general description of the Incident and information to assist individuals in mitigating potential harm, including a customer service number, steps individuals can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.

- Remind individuals of the need to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft.

- Inform each individual about the availability of the Federal Trade Commission's (FTC's) online guidance regarding measures to protect against identity theft and encourage the individual to report any suspected Incidents of identity theft to the FTC and local law enforcement. Provide the FTC's website address and telephone number for the purposes of obtaining the guidance and reporting suspected Incidents of identity theft. At the time of this document's publication, the website address is http://www.ftc.gov/idtheft. The toll-free number for the identity theft hotline is 1-877-IDTHEFT.

Technology Services Assistant Manager and Technology Services Specialists

Contact	Phone	E-Mail
Primary: Brenton Copeland	(940) 498-3251	Brenton.Copeland@cityofcorinth.com
Alternate contact info:	(940) 882-2301 (214) 906-4526	

1. When notified that the IRP has been activated, Technology Services Assistant Manager will collect pertinent information regarding the Incident from the Technology Services Manager and determine the appropriate systems in which to begin inspecting.

2. Inspect server logs and operating system logs. Look for suspicious activity that may suggest the application interface to processing systems was compromised. Look at the operating system level to ensure that servers were not compromised and used as a pass-through into the backend network.

3. Monitor access to database files to identify and alert any attempts to gain unauthorized access. Review appropriate system and audit logs to see if there were access failures prior to or just following the Incident. Other log data should provide information on who touched what file and when. If applicable, review security logs on any non-host device involved (e.g., user workstation).

4. Due to the sensitivity of an Adverse Computer Event or Breach of Sensitive Information, the Technology Services Assistant Manager and Technology Services Specialists will only notify and report findings and work to the following:

   IRT members
   Network Administrator
   Law Enforcement and Forensic Investigators (complying with Texas Business and Commerce Code, Section 521.053)
   Consumer Reporting Agencies (as outlined in 15 U.S.C. Section 1681a)

   The Technology Services Assistant Manager will keep these persons/groups informed throughout the duration of the Incident and its resolution.

5. If credit cardholder data is involved, follow additional steps outlined under Appendix A. Bankcard companies, specifically Visa and MasterCard, have detailed requirements for reporting security Incidents and the suspected or confirmed compromise of cardholder data. Reporting is typically required within 24 hours of compromise.

6. Within 24 hours of notification of an account number compromise, contact the appropriate card companies:

    - Visa Fraud Control Group
    - MasterCard Compromised Account Team
    - Discover Fraud Prevention
    - American Express Merchant Services

7. Act as liaison between the card companies and the Incident Response Team.

8. Ensure credit card companies' specific requirements for reporting suspected or confirmed Breaches of cardholder data are followed. For detailed requirements, see Appendix A.

9. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.

    Note: Visa has specific procedures that must be followed for evidence preservation.

Network Administrator

Contact	Phone	E-Mail
Primary: Jim Norcross	(940) 498-3254	Jim.Norcross@cityofcorinth.com
Alternate contact info:	(940) 882-2307 (682) 365-4248	

1. When notified that the Incident response plan is activated, provide assistance as determined by the details of the reported event.

2. Take measures to contain and control the Incident to prevent further unauthorized access to or use of Sensitive Information, including shutting down particular applications or Third-Party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.

    - Change all applicable passwords for accounts that have access to Sensitive Information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.
    - Do not access or alter the compromised system.
    - Do not turn off the compromised machine. Isolate the system from the network, including unplugging the network cable.
    - Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorized devices that may be using the corporate wireless network.

3. Monitor systems and the network for signs of continued intruder access.

4. Determine if an intruder has exported or deleted any Sensitive Information data.

5. Review firewall logs for correlating evidence of unauthorized access.

6. Determine where and how the Breach occurred.

    - Identify the source of compromise, and the timeframe involved.
    - Review the network to identify all compromised or affected systems. Consider e-commerce Third-Party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected.
    - Document all internet protocol (IP) addresses, operating systems, domain name system names and any other pertinent system information.

7. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.

   Note: Visa has specific procedures that must be followed for evidence preservation.

8. Implement firewall rules as needed to close any exposures identified during the investigation.

Department Director and Manager

Responsibilities

1. Ensure that Technology Services has been notified and a Track-It ticket has been opened.

2. Identify what Sensitive Information may have been compromised. An assumption could be "all" if an entire table or file were compromised.

3. Secure all Sensitive Information that may have been compromised to prevent further access (if able to do so).

4. Upon request from the Incident Response Team, provide detailed information on what Sensitive Information may have be compromised.

Authorized Users

Responsibilities

1. If an Authorized User identifies a possible Adverse Computer Event or Breach of Sensitive Information, contact Technology Services immediately.

2. An Authorized User will assist in the mitigation, investigation, and resolution of an Adverse Computer Event or Breach of Sensitive Information, as needed.

Appendix A

Specific requirements for reporting suspected or confirmed Breaches of cardholder data.

MasterCard Specific Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.

2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail, to compromised_account_team@mastercard.com.

3. Provide the MasterCard Merchant Fraud Control Department with the complete list of all known compromised account numbers.

4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).

5. Provide weekly written status reports to MasterCard, addressing open questions and issues, until the audit is complete to the satisfaction of MasterCard.

6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.

7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs
2. Distribute the account number data to its respective issuers.

Visa U.S.A. Specific Steps:

(Excerpted from Visa U.S.A. Cardholder Information Security Program (CISP), What To Do If Compromised, 3/8/2004)

Refer to documentation online at
http://www.usa.visa.com/media/business/cisp/What_To_Do_If_Compromised.pdf

In the event of a security Breach, the Visa U.S.A. Operating Regulations require entities to immediately report the Breach and the suspected or confirmed loss or theft of any material or records that contain

cardholder data. Entities must demonstrate the ability to prevent future loss or theft of account information, consistent with the requirements of the Visa U.S.A. Cardholder Information Security Program. If Visa U.S.A. determines that an entity has been deficient or negligent in securely maintaining account information or reporting or investigating the loss of this information, Visa U.S.A. may require immediate corrective action.1

If a merchant, or its agent does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Fine the Member Bank
- Impose restrictions on the merchant or its agent, or
- Permanently prohibit the merchant or its agent from participating in Visa programs. 2

Visa has provided the following step-by-step guidelines to assist an entity in the event of a compromise. In addition to the following, Visa may require additional investigation. This includes, but is not limited to, providing access to premises and all pertinent records.3

1 Visa U.S.A. November 2003 Operating Regulations 2.3.F.5
2 Visa U.S.A. November 2003 Operating Regulations 2.3.F.7
3 Visa U.S.A. November 2003 Operating Regulations 2.3.F.3, 2.3.F.4, 2.3.F.5, 2.3.F.6

Steps and Requirements for Compromised Entities

1. Immediately contain and limit the exposure.

    - To prevent further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
        - Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).* 1
        - Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
        - Preserve logs and electronic evidence.
        - Log all actions taken.
        - If using a wireless network, change Service Set Identifier (SSID) on the access point and other machines that may be using this connection (with the exception of any systems believed to be compromised).
        - Be on HIGH alert and monitor all Visa systems.

2. Alert all necessary parties, including:
    - Internal information security group and Incident Response Team, if applicable
    - Legal department
    - Merchant bank
    - Visa Fraud Control Group at (650) 432-2978
    - Local FBI Office U.S. Secret Service – if Visa payment data is compromised

3. Provide the compromised Visa account to Visa Fraud Control Group at (650) 432-2978 within 24 hours.
    - Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.

[3] A person with unlimited access privileges who can perform any and all operations on the computer.

4. Requirements for Compromised Entities
    - All merchant banks must:
        - Within 48 hours of the reported compromise, proof of Cardholder Information Security Program compliance must be provided to Visa.
        - Provide an Incident report document to Visa within four business days of the reported compromise
        - Depending on the level of risk and data elements obtained the following must be completed within four days of the reported compromise:
            - Undergo an independent forensic review
            - A compliance questionnaire and vulnerability scan upon Visa's discretion

Steps for Merchant Banks

1. Contact Visa USA Fraud Control Group immediately at (650) 432-2978
2. Participate in all discussions with compromised entity and Visa USA
3. Engage in a Visa approved security assessor to perform the forensic investigation
4. Obtain information about compromise from the entity
5. Determine if compromise has been contained
6. Determine if an independent security firm has been engaged by the entity
7. Provide the number of compromised Visa accounts to Visa Fraud Control Group within 24 hours
8. Inform Visa of investigation status within 48 hours
9. Complete steps necessary to bring entity into compliance with CISP according to timeframes described in "What to do if Compromised"
10. Ensure that entity has taken steps necessary to prevent future loss or theft of account information, consistent with the requirements of the Visa USA Cardholder Information Security Program

Forensic Investigation Guidelines

Entity must initiate investigation of the suspected or confirmed loss or theft of account information within 24 hours of compromise.

The following must be included as part of the forensic investigation:

1. Determine cardholder information at risk.
    a. Number of accounts at risk, identify those stored and compromised on all test, development, and production systems

b. Type of account information at risk
c. Account number
d. Expiration date
e. Cardholder name
f. Cardholder address
g. CVV2[2]
h. Track 1 and Track 2[3]
i. Any data exported by intruder

2. Perform Incident validation and assessment.

    a. Establish how compromise occurred
    b. Identify the source of compromise
    c. Determine timeframe of compromise
    d. Review entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development, and production environments as well as VPN, modem, DSL and cable modem connections, and any Third-Party connections.
    e. Determine if compromise has been contained.

3. Check all potential database locations to ensure that CVV2, Track 1 and Track 2 data are not stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.).

4. If applicable, review VisaNet endpoint security and determine risk.

5. Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed.

6. Perform remote vulnerability scan of entity's Internet facing site(s)

Visa Incident Report Template

This report must be provided to Visa within 14 days after initial report of Incident to Visa. The following report content and standards must be followed when completing the Incident report. Incident

[2] CVV2 is an authentication process established by credit card companies to further efforts towards reducing fraud for Internet transactions. It consists of requiring a card holder to enter the CVV2 number at transaction time to verify that the card is on hand. This number is printed on MasterCard & Visa cards in the signature area of the back of the card. (it is the last 3 digits AFTER the credit card number in the signature area of the card).

[3] Track 1 is a "track" of information on a credit card that has a 79-character alphanumeric field for information. Normally a credit card number, expiration date and customer name are contained on track 1. Track 2 is a "track" of information on a credit card that has a 40- character field for information. Normally a credit card number and expiration date are contained on track 2.

report must be securely distributed to Visa and Merchant Bank. Visa will classify the report as "Visa Secret" *.

I. Executive Summary
   a. Include overview of the Incident
   b. Include Risk Level (High, Medium, Low)
   c. Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures
   a. Include forensic tools used during investigation

V. Findings
   a. Number of accounts at risk, identify those stored and compromised
   b. Type of account information at risk
   c. Identify ALL systems analyzed. Include the following:
      i. Domain Name System (DNS) names
      ii. Internet Protocol (IP) addresses
      iii. Operating System (OS) version
      iv. Function of system(s)
   d. Identify ALL compromised systems. Include the following:
      i. DNS names
      ii. IP addresses
      iii. OS version
      iv. Function of system(s)
   e. Timeframe of compromise
   f. Any data exported by intruder
   g. Established how and source of compromise
   h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.).
   i. If applicable, review VisaNet endpoint security and determine risk.

VI. Compromised Entity Action

VII. Recommendations

VIII. Contact(s) at entity and security assessor performing investigation

* This classification applies to the most sensitive business information, which is intended for use within Visa. Its unauthorized disclosure could seriously and adversely impact Visa, its employees, member banks, business partners, and/or the Brand.

Discover Card Specific Steps:

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102.

2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.

3. Prepare a list of all known compromised account numbers.

4. Obtain additional specific requirements from Discover Card.

American Express Specific Steps:

1. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200.

2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.

3. Prepare a list of all known compromised account numbers.

4. Obtain additional specific requirements from American Express.

CITY OF CORINTH

POLICY/ADMINISTRATIVE PROCEDURE/ADMINISTRATIVE DIRECTIVE

SECTION:	TECHNOLOGY SERVICES	REFERENCE NUMBER:
SUBJECT:	POLICY	EFFECTIVE DATE 03/01/2020
TITLE:	COMPUTER AND SENSITIVE INFORMATION INCIDENT RESPONSE PLAN	*LAST REVISION DATE:* 03/01/2020

1.0 PURPOSE

The purpose of this Policy is to establish the goals and the vision for the computer and sensitive information Incident Response Plan. This Policy will clearly define to whom it applies and under what circumstances, and it will include the definition of an Incident, Staff Member roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. This Policy shall be well-publicized and made easily available to all personnel whose duties involve data privacy and security protection.

By publishing a Computer and Sensitive Information Incident Response Plan, the City of Corinth Technology Services (TS) Department seeks to focus significant attention on network and data security. This Policy strives to protect City of Corinth, its Staff Members, Third-Parties, and the public from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.0 DEFINITIONS

2.1 Adverse Computer Event – An event with a negative consequence to an information systems network, such as: unauthorized use of system privileges, unauthorized access to Sensitive Information/Data, or execution of malware that destroys data or holds it for ransom.

2.2 Breach – An event in which sensitive information is released or exposed to an unsecure environment, or an untrusted recipient.

2.3 City – City of Corinth, Texas.

2.4 City Council – The elected legislative body of the City of Corinth, Texas.

2.5 City Manager – The person appointed as the City Manager of the City of Corinth, Texas.

2.6 Director – An employee designated by the City Manager as a director-level position.

2.7 Encrypted Data – Any file, database, or information that has undergone Encryption.

2.8 Encryption – A process by which data is safeguarded by encoding it so that only the authorized parties can access it.

2.9 Incident – An event in which the integrity of Sensitive Information/Data is compromised, either intentionally or coincidentally.

2.10 Incident Response Plan – The guidelines by which City Staff, Contractors, and Third-Parties must abide during an Incident.

2.11 Personal Identifiable Information (PII) – Any data that could potentially identify a specific individual (e.g., Social Security Numbers, Driver's License Numbers, etc.). Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered.

2.12 Proprietary Information – Information that could reasonably be expected to be guarded from public knowledge. This could include information about Staff Members, the public, or other information about official City business that is not subject to Open Records.

2.13 Protected Health Information (PHI) – Under US law, any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

2.14 Sensitive Information/Data – Information or data, Encrypted or not, whose content requires that the security and integrity of the data are not compromised. This Data must be protected against unauthorized access. It may contain PII, PHI, financial data (such as credit card information or bank account numbers), or other Proprietary Information.

2.15 Staff Member – Any part-time or full-time employee, contract employee, temporary employee, City Council member, or volunteer doing business in an official capacity on behalf of the City.

2.16 Third-Party – An outside firm or individual with whom the City is contracting for services.

3.0 PROCEDURE

3.1 Preface – The City of Corinth has established this Policy to ensure the security of its Sensitive Information/Data, outline the roles and responsibilities of Staff Members and Third-Parties, and how to respond to an Incident. This is achieved by the formal adoption of the Incident Response Plan (attached) by the City Council. The City intends to honor the policies set forth, but reserves the right to change the requirements at any time with City Council approval.

3.2 A Staff Member is required to notify Technology Services at any moment they suspect there might be an Incident compromising the integrity of Sensitive Information/Data. This requirement stands irrespective of the Staff Member's involvement in the Incident. That is to say, simply overhearing details of an Incident compels the Staff Member to notify Technology Services.

3.3 Notifying Technology Services can be made through any of these means:

3.3.1 Calling the Help Desk phone number: (940) 498-3205. Should the phone call go to voicemail, a voice message will be left, detailing the time and nature of the Incident.

3.3.2 Entering a new ticket in the Technology Services' Track-It system, detailing the time and nature of the Incident.

3.3.3 Emailing Technology Services: TechnologyServices@cityofcorinth.com, detailing the time and nature of the Incident.

3.4 The three preceding methods of notification are monitored by TS Staff Members. Upon receiving the notification, the responding TS Staff Member may contact the Notifying Staff Member for clarification, then relay the information to the TS Manager.

3.5 Working with the Director of Finance, Communications, and Strategic Services, the TS Manager will initiate and follow the Incident Response Plan (attached).

3.6 Staff Members will be periodically updated during the Incident by the Incident Response Team (IRT). Once the Incident has been resolved, the IRT will send an all-clear to Staff Members.

3.7 Scope – Understanding that simply having computer access is not necessary to put the City's Sensitive Information/Data at risk, this Policy applies to all Staff Members, regardless of what, if any access they have to the City's computer network.

4.0 VIOLATION

4.1 Any Staff Member found to have willfully obfuscated or impeded the investigation will be subject to disciplinary action, up-to and including termination.

4.2 If the results of the Incident investigation determined that a Staff Member knew of the potential of an Adverse Computer Event, but did not inform Technology Services, that Staff Member will be subject to disciplinary action, up-to and including termination.

4.3 If the results of the Incident investigation determine that the actions of a Staff Member directly or indirectly led to the Adverse Computer Event, that Staff Member will be subject to disciplinary action, up-to and including termination.

5.0 MODIFICATIONS

5.1 The City Council authorizes the City Manager to alter the Incident Response Team contact information, as well as Incident Response Team composition as he or she sees fit.

5.2 All other substantial changes to the Incident Response Plan or associated Policy must be approved by the City Council.

Adverse Computer Event Report

REPORTED BY: _____ DATE OF REPORT: _____

TITLE / ROLE: _____ INCIDENT NO.: _____

INCIDENT ASSESSMENT: NEGLIGIBLE: ☐ MINOR: ☐ SIGNIFICANT: ☐ CRITICAL: ☐

INFORMATION SECURITY INCIDENT INFORMATION

DATE OF INCIDENT: _____ TIME OF INCIDENT: _____

INCIDENT POC: _____ TITLE / ROLE: _____

PHONE: _____ EMAIL: _____

LOCATION: _____

SPECIFIC AREA OF LOCATION *(if applicable)*: _____

INCIDENT TYPE: _____

NO. OF HOSTS AFFECTED: _____ SOURCE IP ADDRESS: _____

IP ADDRESSES: _____ COMPUTER / HOST: _____

OPERATING SYSTEMS: _____ OTHER APPLICATIONS: _____

INCIDENT DESCRIPTION:

IMPACT ASSESSMENT:

RESULTING DAMAGE:

IMMEDIATE ACTION TAKEN:

PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:

ADDITIONAL INFORMATION:

INFORMATION SECURITY INCIDENT INFORMATION SHARING		
DEPARTMENT REQUIRING NOTIFICATION	POINT OF CONTACT NAME	DATE OF NOTIFICATION

REPORTING STAFF NAME: _____ **REPORTING STAFF SIGNATURE:** _____ **DATE:** _____

SUPERVISOR NAME: _____ **SUPERVISOR SIGNATURE:** _____ **DATE:** _____

BUSINESS ITEM 5.

City Council Regular and Workshop Session

Meeting Date:	02/20/2020		
Title:	Corinth and Dallas Off-Road Bicycle Association (DORBA) Trails Use Agreement		
Submitted For:	Cody Collier, Director	**Submitted By:**	Cody Collier, Director
Finance Review:	N/A	**Legal Review:**	Yes
City Manager Review:	**Approval:** Bob Hart, City Manager		
Strategic Goals:	Infrastructure Development Citizens Engagement &Proactive Government Regional Cooperation		

AGENDA ITEM

Consider authorzing the city manager to execute a memorandum of agreement between the CIty of Corinth and the Dallas Off-Road Bicycle Association (DORBA), for the use and maintenance of Corinth trails.

AGENDA ITEM SUMMARY/BACKGROUND

Corinth staff and the Dallas Off-Road Bicycle Association (DORBA) have been collaborating for a mutually beneficial agreement for trails use and maintenance. DORBA is well established in the North Texas and have several use agreements with cities across the region. DORBA asks for permission to use the trails for recreational purposes which conform to Corinth's trails requirements including: no motorized vehicles, no use days due to rain or dangerous conditions, and our standard park hours. In return, DORBA will provide a Corinth citizen interested in becoming the "Trail Steward" and provide all maintenance for the trial system.

The Trail Steward will provide regular inspections of the trail, post signs indicating whether the trails are open or closed, and work with Corinth staff regarding maintenance tasks. DORBA will provide all volunteer labor, tools, equipment and funds to perform any required maintenance activities, and coordinate with Corinth prior to performing these duties and for final inspection for acceptance from Corinth. All improvements or structures created by DORBA will be done through a permit/ inspection process and will become Corinth property upon completion.

Corinth Parks and Recreation Board members met with DORBA, discussed intent, and reviewed DORBA's contract agreement. the Board is in favor of entering into an agreement with DORBA and entering into a partnership.

RECOMMENDATION

Staff recommends approval of the Memorandum of Agreement between the Dallas Off-Road Bicycle Association and Corinth.

Attachments

Corinth/ DORBA MOU

DORBA (www.DORBA.org)
Dallas Off-Road Bicycle Association
PMB 619
6333 E. Mockingbird Suite 147
Dallas, TX 75214-2692

MEMORANDUM OF AGREEMENT

The ***LANDOWNER*** ("OWNER") and the ***DALLAS OFF-ROAD BICYCLE ASSOCIATION*** ("DORBA"), each organization acting by and through duly authorized officers, enter into the following Use Agreement this the_____day of_____, 2008.

WHEREAS, DORBA, a Texas non-profit corporation, seeks to promote and provide off-road riding opportunities and related activities for its membership and has successfully cooperated with other governmental agencies in accomplishing trail projects; and

WHEREAS, **OWNER** has developed public facilities at a facility to be named in THIS LOCATION and desires to maintain a single-track, mixed use trail with the support from volunteers and trail users; and

WHEREAS, **OWNER** and DORBA desire to form a trail support group advocating the proper design, construction, maintenance and use of public hike and bike single-track, mixed use trails within THIS LOCATION; and

WHEREAS, DORBA agrees to enter into a partnership with **OWNER** to help design, construct and maintain a trail for the purpose of recreational riding, racing under strict supervision, hiking, jogging, ecological and environmental awareness training, and future goodwill.

NOW, THEREFORE, for and in consideration of the premises and mutual benefits thereof, the parties hereto agree as follows:

ARTICLE 1.0 VOLUNTEERS

1.1 NOTIFICATION

DORBA shall submit to **OWNER** a list of volunteer workers ("Volunteers") following any trail work. OWNER staff shall be notified of scheduled DORBA workdays and shall allow Volunteers free access into designated work areas.

All proposed trail modifications shall be reviewed and approved by OWNER staff and DORBA Vice-President of Trails and Advocacy prior to initiating work activities. OWNER staff shall be notified of routine trail maintenance activities required to keep the trail open and safe. Specific work activities shall be coordinated with the OWNER or their designee. An accurate summary of all work activities and number of volunteer hours shall be submitted by DORBA to OWNER or their designee.

DORBA (www.DORBA.org)
Dallas Off-Road Bicycle Association
PMB 619
6333 E. Mockingbird Suite 147
Dallas, TX 75214-2692

1.2 PROTECTIVE CLOTHING

For optimum safety, the use of protective eye wear, head protection, gloves, hard-soled or steel-toed shoes and long sleeved shirts as appropriate for the specific work task shall be required by all Volunteers. Certain conditions or activities may require the use of dust masks.

1.3 LIABILITY, INDEMNIFICATION AND INSURANCE

All DORBA Volunteers shall sign a Waiver of Liability releasing OWNER and its officers and employees from all liability for personal injury or damage to personal property incurred while participating in this project.

DORBA shall indemnify and hold harmless OWNER and its officers and employees from all suits, actions, losses, damages, claims, or liability of any character, type, or description, including, but not limited to, all expenses of litigation, including attorneys' fees, court costs and penalties, of any kind or nature, arising, directly or indirectly, from the existence, operation and/or enforcement of this Agreement, or arising from any actions or inactions of DORBA, its agents, servants, employees or Volunteers.

Prior to execution of this Agreement, DORBA shall provide OWNER with proof of general liability coverage in a minimum amount of One Million and No/100 Dollars ($1,000,000.00) aggregate. OWNER shall be named as an additional insured, if required by the OWNER and submitted to DORBA in writing prior to the execution of this document, with regard to the foregoing. In the event that DORBA hires workers directly or enters into a contract for work to be performed on the trail, DORBA will provide OWNER with proof of Worker's Compensation coverage for such personnel performing the work. Any change in any policy or coverage shall be subject to the prior written approval of OWNER.

In the instance where an event is held on the trail by a promoter other than DORBA, prior to the issuance of a permit by the LANDOWNER, the promoter shall provide:

1. A Certificate of Insurance listing DORBA as additionally insured;
2. A document that specifies the time and location they will be meeting with the DORBA Trail Steward to assess, fix, and/or repair any damage that has occurred to the trail during the event.

All DORBA Volunteers shall have a Waiver of Claim on file releasing DORBA from any and all claims of damage due to participation in DORBA-sponsored events.

DORBA (www.DORBA.org)
Dallas Off-Road Bicycle Association
PMB 619
6333 E. Mockingbird Suite 147
Dallas, TX 75214-2692

ARTICLE 2.0 GENERAL

2.1 CONSTRUCTION MATERIALS

All materials used in construction shall be furnished by DORBA, unless other arrangements have been agreed to by both parties. OWNER shall retain ownership of any materials installed on the trail.

Natural materials such as rocks, logs, etc. shall be used in trail construction only with the approval of the OWNER, their designee, or by the Trail Steward or other DORBA Officer as done in conformance with IMBA Guidelines and Recommendations[1]. No natural materials shall be removed from the facility by DORBA Volunteers without written approval from the Parks Director. No trees shall be removed or significantly pruned without the written approval of the Parks and Recreation Director in consultation with the OWNER Arborist.

If any structures are built (examples include land bridges, suspended bridges, ramps, etc) after the execution of this document, they will make every attempt to use the following guidelines for construction:

1. All connections should be done with min. 3/8 in through bolts with flat washers on both OWNERes, and lock washer.
2. If through bolts are not possible in some connections, then 3/8 in. lag bolts are acceptable with flat washers installed. Length of bolts should be at least ¾ of the combined thickness of the connection.
3. Any fasteners visible to the tread surface, shall be counter sunk into the surface material so that they are flush or recessed.
4. If 2x6 lumber is used for the tread, then 3.0 in deck screws shall be acceptable for fastening to the substructure. Two screws per contact point with substructure shall be used.
5. Tread surface shall be a minimum of 4.0 ft wide
6. Tread shall be spaced at least 0.5 in and max of 2.0 in apart.
7. Any lumber used shall be pressure treated or equivalent so as to withstand exterior exposure conditions. No interior framing lumber shall be used at any time on any part of the structure.

[1] International Mountain Biking Association, *Trail Solutions, IMBA's Guide to Building Sweet Singletrack*, 2004. International Mountain Biking Association, P.O. Box 7578, Boulder, Colorado, 80306, www.imba.org

8. If handrail is used, must be a minimum of 3.0 ft to top rail height as measured from the tread surface.
9. 4x4 anchor posts must be embedded into ground a minimum of 4.0 ft, and hole to be backfilled with compacted earth in 1.0 in lifts, or 3000psi concrete. If concrete is used as anchor material, the hole shall be a minimum of 12.0 in in diameter so to provide proper spacing and consolidation.
10. Inboard and outboard slopes for entry and exit shall not exceed 1:4.
11. Entry and exit ramps shall be embedded into ground at least 6.0 in for stability.

Any deviations for construction needed to accommodate in field conditions shall be approved through VP of Trails and Advocacy, or Trail Steward in writing, and submitted to the DORBA Secretary.

2.2 TOOLS/EQUIPMENT/STORAGE

DORBA Volunteers shall be responsible for their own tools. OWNER staff will provide specialty tools and equipment at its sole discretion. OWNER Staff shall be responsible for all OWNER equipment and shall directly supervise its use.

2.3 DISPOSAL

DORBA shall coordinate with OWNER staff for the removal and on-site disposal of unwanted construction materials or waste. DORBA Volunteers are responsible for removing their own trash and litter.

2.4 SUPERVISION

An OWNER representative may be present to supervise trail work activities. This representative shall be furnished with two-way communications equipment to facilitate work activities and aid in any emergencies. It is understood that OWNER representative has legal authority over the entire work party.

DORBA shall designate a Trail Steward, other appointed DORBA member, or DORBA Board member to lead and be responsible for each work party. This Trail Steward, other appointed DORBA member, or DORBA Board member shall organize the Volunteers, keep necessary written records, and account for all DORBA-owned equipment and tools.

2.5 VOLUNTEER TRAIL PATROLS

To promote responsible use of the trails and to enhance public/private cooperation, Volunteers are invited to patrol the trails with commissioned OWNER personnel. Trail Steward, other appointed DORBA member, or DORBA Board member will assist in scheduling and promotion of the trail patrol program.

2.6 MODIFICATION OF AGREEMENT

This Agreement may be amended by written proposal signed by authorized agents of both OWNER and DORBA. All amendments shall bear the conditions and intent of the original Agreement, unless specifically noted otherwise.

2.7 TERM

The term of this Agreement shall be indefinite. The parties understand and agree that OWNER is funded on an annual fiscal basis, and any payment due and owing after the current fiscal year is subject to an annual appropriation by OWNER Council. In the event appropriations are not made to cover this Agreement, this Agreement shall expire without further obligations of either party.

2.8 TERMINATION OF AGREEMENT

DORBA or the OWNER may challenge the Agreement in writing which challenge must be resolved within thirty (30) days with a newly signed Agreement or the Agreement is terminated. Either party may terminate this Agreement upon thirty (30) days prior written notice to the other. Upon termination, all improvements constituting the Erwin Park trail shall remain in place and become OWNER property. However, OWNER may, within its sole discretion, require DORBA to return Erwin Park to its original condition.

2.9 BUDGET

DORBA shall be responsible for all costs of trail maintenance unless OWNER has reasonably adequate advance notice of trail maintenance costs and has funds budgeted to contribute to the costs

2.10 MISCELLANEOUS

If any provision or term of this Agreement is judicially determined to be invalid, void or unenforceable for any reason, the remainder of this Agreement shall remain valid and

enforceable and shall in no way be affected, impaired or invalidated if the same may be given effect without the void or invalid provision.

This Agreement shall be interpreted in accordance with and shall be governed by the laws of the State of Texas. This Agreement is performable in Collin County, Texas, and the parties agree that venue from any disputes affecting the Agreement shall be in Collin County, Texas.

Any notice or other communication hereunder shall be in writing, shall be sent via registered or certified mail, and shall be deemed given when deposited, postage prepaid, in the United States mail, addressed as set forth below, or to such other address as either of the parties shall advise the other in writing:

If to DORBA:

Dallas Off Road Bicycle Association
PMB 619
6333 E. Mockingbird, Suite 147
Dallas, Texas 75214-2692
Attention: Club PreOWNERent

If to OWNER:
OWNER
P. O. Box 12345
Somewhere, Texas 75069
Attention: John Doe, Director of Parks and Recreation

This Agreement or any part hereof shall not be assigned or otherwise transferred by either party without the prior written consent of the other party.

DORBA (www.DORBA.org)
Dallas Off-Road Bicycle Association
PMB 619
6333 E. Mockingbird Suite 147
Dallas, TX 75214-2692

ARTICLE 3.0 CONCLUSION

IT IS HEREBY UNDERSTOOD AND AGREED by both parties that the sole purpose of this Agreement is to create and maintain a system of trails at a park to be name by OWNER RICHARDSON which will benefit both parties. All Rules and Regulations of DORBA, the OWNER and its Parks Department shall be observed and followed.

IN WITNESS HEREOF, the parties have executed this Agreement on this the_____day of _____, 2009.

OWNER	***DALLAS OFF-ROAD BICYCLE ASSOCIATION***
John Doe OWNER Manager	Rich Szecsy Club President 2009

BUSINESS ITEM 6.

City Council Regular and Workshop Session

Meeting Date: 02/20/2020
Title: Classic Mazda Sign Application
Submitted For: Helen-Eve Liebman, Director
Submitted By: Cleve Joiner, Building Official
Finance Review: N/A **Legal Review:** N/A
City Manager Review:
Strategic Goals: Land Development
Economic Development

AGENDA ITEM

Consider and act on a request by Classic Mazda Company for an application to the Unified Development Code Section 4.01.15. General Requirements – Section E – 3. Maximum Height, Section E – 4 Maximum Sign Area and E- 5 Maximum Sign Structure Area. The request is to allow certain increases to the monument sign allowed by ordinance requiring City Council approval. The sign being replaced is located at 5000 S. I35E along the I-35E frontage, legally described as Lot 1, Blk A of the Classic Mazda Addition, City of Corinth, Denton County, Texas.

AGENDA ITEM SUMMARY/BACKGROUND

Classic Mazda is proposing to replace their current pole sign with a new Mazda corporate model monument sign complementing the significant remodel of the facility. The new sign is eleven (11) feet shorter in height and three (3) square feet less in sign area than the existing sign. City ordinance allows the City Council to approve greater height and areas for signs. In addition to the approval there are three (3) required performance-based enhancements. The proposed replacement sign meets five (5) of the eight (8) enhancements defined by the City of Corinth Code of Ordinances. The five performance-based enhancements Classic Mazda is offering for the sign allowances include architectural materials, features, and design matching the main building, as well as contrasting sign colors, and simple font styles with limited text or logo.

SIGN MEASUREMENTS	CURRENT SIGN	PROPOSED SIGN	COUNCIL APPROVAL
HEIGHT	41 FEET	30 FEET	30 FEET
SIGN AREA PER SIDE	105 SF	102 SF	300 SF
SIGN STRUCTURE PER SIDE	212 SF	316.4 SF	320 SF

The summary of existing, proposed, and City Council's height and area approval authority is included in the detailed attachment.

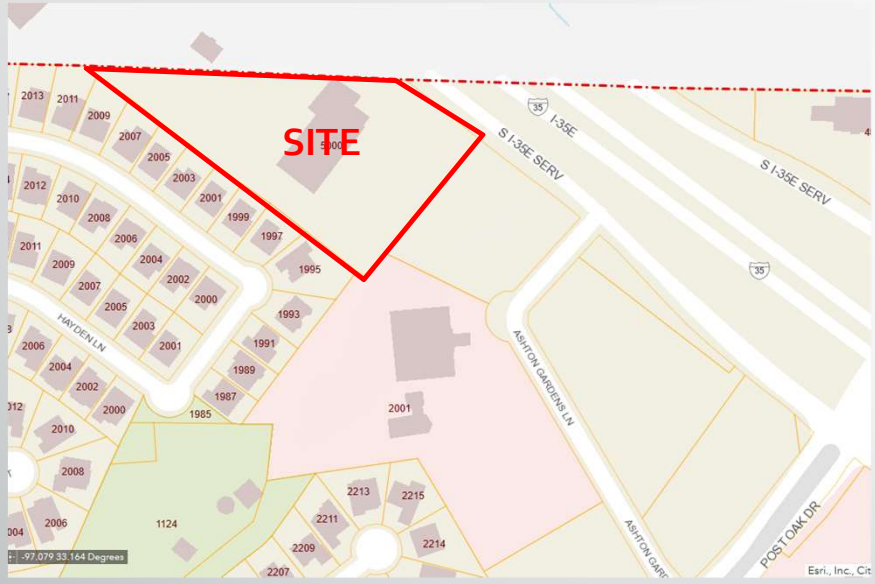
RECOMMENDATION

Staff Recommendation is to approve the application for the new monument sign.

Attachments

Classic Sign

Classic Mazda – Monument Sign



Classic Mazda – Monument Sign

Classic Mazda – Monument Sign

SIGN MEASUREMENTS	CURRENT	PROPOSED	BASE SIGN REQUIREMENTS	CITY COUNCIL INCREASE APPROVAL Plus Three Performance Based Enhancements
Height	41 Feet	30 Feet	8	30 Feet
Sign Area Per Side	105 Square Feet	102 Square Feet	80	300 Square Feet
Sign Structure Area Per Side	212 Square Feet	316.4 Square Feet	100	320 Square Feet

Classic Mazda – Monument Sign

Section 4.01.15 General Requirement s

The City Council may approve a sign height up to thirty (30) feet, sign area up to three hundred (300) Square feet and three hundred-twenty (320) square feet of sign structure if the sign has a minimum of three (3) performance-based enhancements

1. Architectural Materials – Matching the Building
2. Architectural Features - Matching the Building
3. Architectural Design - Matching the Building
4. External Lighting, Shielded, Directed, Spotlight Fixtures
5. Landscape Ratio of Greater than 1:1 for Ground Area to Sign Area
6. Contrasting Sign Colors
7. Simple Font Styles with Limited Text or Logos
8. Specific Panel Size for Individual Tenants

CORINTH
TEXAS

Classic Mazda – Monument Sign

* Staff Recommendation is for City Council Approve the Application for the New Monument Sign.