RESOLUTION NO. 003-2020

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF BIG SPRING, TEXAS, ADOPTING THE SECURITY AWARENESS POLICY OF THE CITY OF BIG SPRING; AUTHORIZING THE CITY MANAGER OR HIS DESIGNEE TO TAKE SUCH STEPS AS ARE NECESSARY TO IMPLEMENT SAID POLICY; AND PROVIDING AN EFFECTIVE DATE

WHEREAS, the City Council finds it necessary to implement a Security Awareness Policy pursuant to H.B. 3834, which mandates that local government entities conduct annual cyber-security training for all employees who have access to a local government computer system or database and elected officials regardless of their access to a local government computer system or database; and

WHEREAS, cyber-security training has been initiated and the City is on track to complete training by the June 14, 2020 deadline; and

WHEREAS, the Information Technology (IT) and Human Resources (HR) Departments have reviewed this policy and recommend its approval;

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF BIG SPRING, TEXAS, THAT:

SECTION 1. The City Council hereby adopts the "City of Big Spring Security Awareness Policy," attached as Exhibit A, and incorporated herein as if copied verbatim.

SECTION 2. The City Manager or his designee shall ensure that these policies and procedures are implemented.

SECTION 3. Any prior resolution that is inconsistent with this resolution is hereby repealed and declared to be of no further force or effect.

SECTION 4. This resolution shall be effective immediately upon approval on second reading pursuant to the Big Spring City Charter.

PASSED AND APPROVED on first reading at a regular meeting of the City Council on the **25th** day of **February**, **2020** with all members of the Council voting "aye" for the passage of same.

PASSED AND APPROVED on second and final reading at a regular meeting of the City Council on the **10th** day of **March**, **2020** with all members of the Council voting "aye" for the passage of same.

Shannon D. Thomason, Mayor

ATTEST:

Tami L. Davis, Assistant City Secretary

BIG SPRING
TEXAS

Security Awareness Policy

Document History

Rev #	Name	Date	Description
1.0	Miklos Szabo	12/04/2019	Initial draft
1.1	Legal Dept.	02/21/2020	Council Consideration
1.2	Council	2/25/2020	Council Approval

Res. 003-2020

Table of Contents

1. Introduction

Technical security controls are a vital part of our information security framework but are not in themselves sufficient to secure all information assets. Effective information security also requires the awareness and proactive support of all employees, officials, Council members and Contractors, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks and other current exploits being used, which specifically target vulnerable humans rather than IT and network systems.

Lacking adequate information security awareness, a member is less likely to recognize or react appropriately to information security threats and incidents are more likely to place information assets at risk of compromise. In order to protect information assets, all authorized users of the local government computer systems or databases, Councilmembers, and contractors must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations.

1.1 Objective

This policy specifies the City of Big Spring Security Awareness and Training Program to inform, assess, train, and remediate all Members regarding their information security obligations.

1.2 Scope

This policy applies throughout the organization as part of the corporate governance framework. It applies to City of Big Spring employees, managers, directors, administrators, councilmembers, officials and contractors with access to the local government computer systems, network, databases, company information, confidential personal information, personally identifiable information, and/or customer data. This policy also applies to third party employees working for the organization whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

For the purposes of this policy the term "Member" or "Members" shall mean any City of Big Spring employee, manager, director, administrator, or Councilmember, official, or contractor that has been authorized as a user of the local government computer systems, network, databases, company information, confidential personal information, personally identifiable information, or those who may handle customer data.

1.3 Document Changes and Feedback

This policy will be reviewed and updated as needed to reflect, among other things, changes to applicable law, update or changes to City of Big Spring requirements, technology, and the results or findings of any audit.

1.4 Referenced Documents

Documents that are relevant to this policy include the following:

Policy	Policy Owner	Document Location
City of Big Spring Handbook/Personnel Policies	City of Big Spring	Human Resources
City of Big Spring Directives	City of Big Spring/City Manager	Human Resources
IT Acknowledgment and Agreement	City of Big Spring	Human Resources

KnowBe4 Security Awareness Training	KnowBe4	Administered by Information Technology Manager

2. Policy Requirements

All awareness training must fulfill the requirements for the security awareness program as listed below:

- The information security awareness program should ensure that all Members achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.

- Additional training is appropriate for Members with specific obligations towards information security that are not satisfied by basic security awareness, as determined by the IT Manager, or have failed completion of an assigned course. Such training requirements must be identified in departmental/personal training plans and funded accordingly. The training requirements will reflect relevant prior experience, training and/or professional qualifications, as well as anticipated job requirements.

- Security awareness and training activities should commence as soon as practicable after a Member join the organization, generally through assigned training activities assigned by the IT Manager. The training activities should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.

- Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is so important, but the motivators may be different for those individuals focused on their own duties or managers with broader responsibilities to the organization and their staff.

- The City of Big Spring Human Resources (HR) and Information Technology (IT) Departments will provide information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters.

2.1 City of Big Spring Information Security Awareness Training

The City of Big Spring Information Technology (IT) department requires that each Member, upon hire and at least annually thereafter, successfully complete all assigned Security Courses. Certain Members may be required to complete additional training modules depending on their specific job requirements. All Members will be given a reasonable amount time to complete each course so as to not disrupt business operations.

2.2 Simulated Social Engineering Exercises

The City of Big Spring IT department will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. The City of Big Spring IT department will conduct these tests at random throughout the year with no set schedule or frequency. The City of Big Spring IT department may conduct targeted exercises

against specific departments or individuals based on a risk determination.

2.3 Remedial Training Exercises

From time to time, City of Big Spring Members may be required to complete remedial training courses or may be required to participate in remedial training exercises with the City of Big Spring IT Department as part of a risk-based assessment.

3. Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for all Members. The City of Big Spring IT Department will monitor compliance and non-compliance with this policy and report to the City Manager the results of training and social engineering exercises.

The penalties for non-compliance are described in Appendix A of this policy.

3.1 Non-Compliance Actions

Certain actions or non-actions by Members may result in a non-compliance event (Failure).

A Failure includes but is not limited to:

- Failure to complete required training within the time allotted
- Failure of a social engineering exercise

Failure of a social engineering exercise includes but is not limited to:

- Clicking on a URL within a phishing test
- Replying with any information to a phishing test
- Opening an attachment that is part of a phishing test
- Enabling macros that are within an attachment as part of a phishing test
- Allowing exploit code to run as part of a phishing test
- Entering any data within a landing page as part of a phishing test
- Transmitting any information as part of a vishing test
- Replying with any information to a smishing test
- Plugging in a USB stick or removable drive as part of a social engineering exercise
- Failing to follow company policies in the course of a physical social engineering exercise

Certain social engineering exercises can result in multiple Failures being counted in a single test. The maximum number of Failure events per social engineering exercise is two (2).

The City of Big Spring IT Department may also determine, on a case by case basis, that specific Failures are a false positive and should be removed from that member's total Failure count.

3.2 Compliance Actions

Certain actions or non-actions by members may result in a compliance event (Pass).

A Pass includes but is not limited to:

- Successfully identifying a simulated social engineering exercises
- Not having a Failure during a social engineering exercise (Non-action)
- Reporting real social engineering attacks to the IT department by utilizing the Phishing Alert Report

button in outlook, or on other approved email programs.

3.3 Removing Failure Events through Passes

Each Failure will result in a Remedial training or coaching event as described in Appendix A of this document. Subsequent Failures will result in escalation of training or coaching. De-escalation will occur when three consecutive Passes have taken place.

4. Responsibilities and Accountabilities

Listed below is an overview of the responsibilities and accountabilities for managing and complying with this policy program.

The Information Technology (IT) Manager is accountable for running an effective information security awareness and training program that informs and motivates Members to help protect the organization's and the organization's customer's information assets.

The Information Technology (IT) Manager is also responsible for developing and maintaining a comprehensive suite of information security policies (including this one), standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. Working in conjunction with other corporate functions, it is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of Member's responsibilities identified in applicable policies, laws, regulations, contracts, etc.

All Directors are responsible for ensuring that their staff and others within their responsibility participate in the information security awareness, training, and educational activities where appropriate and required.

All Members are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations at all times.

Appendix A – Schedule of Failure Penalties

The following table outlines the penalty of non-compliance with this policy. Steps not listed here may be taken by the City of Big Spring IT team to reduce the risk that a Member may pose to the company.

Failure Count	**Resulting Level of Remediation Action**
First Failure	Mandatory completion of failed course.
Second Failure	Mandatory completion of failed course.
Third Failure	Mandatory completion of failed course.
Fourth Failure	Meeting with Department Manager
Fifth Failure	Meeting with Department Manager and Human Resources Director
Subsequent Failures	Meeting with Department Manager and Human Resources Director - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events - Formal review of employment with Human Resources Director - Potential for Termination of Employment or Employment Contract

Appendix B – Methods for Determining Staff Risk Ratings

The following is a list of situations that may increase a risk rating of a City of Big Spring Member. Higher risk ratings may result in an increased sophistication of social engineering tests and an increase in frequency and/or type of training and testing.

- Member email resides within a recent Email Exposure Check report
- Member is an executive or VP (High value target)
- Member possesses access to significant company confidential information
- Member is using a Windows or Apple-based operating system
- Member uses their mobile phone for conducting work-related business
- Member possesses access to significant company systems
- Member personal information can be found publicly on the internet
- Member maintains a weak password
- Member has repeated company policy violations