

## CITY OF PLANO POLICIES AND PROCEDURES

532.000

**Department Name:** Technology Services  
**Procedure:** Vendor and Contractor Network Security Policy

**Effective Date:** 1/1/2005  
**Revision Date(s):** 12/14/2005, 1/18/2006  
**Review: Annual:** 8/1/2006

### I. Purpose

The purpose of this policy is to create an environment within the City that maintains system security, data integrity, and privacy while preventing unauthorized access to misuse of, damage to, or loss of data. It is the intent of the City that all City vendors will adhere to the policies identified in this document and City of Plano Policies and Procedures 223 and 224. This policy is the City's vehicle for emphasizing the commitment to network security and making clear the expectations for vendor involvement and accountability.

### II. Policy

These policies and procedures shall apply to all vendors.

### III. System Authorization

- A. Each vendor is responsible for actions taken with their network, computer, and logon accounts.
- B. Access to City of Plano computer resources is restricted on a "need to access" basis. That is, access is allowed only to fulfill authorized City of Plano responsibilities.
- C. Vendors using the City's computer systems must not use these facilities for illegal activities, for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by City management.
- D. Vendors must not test or attempt to compromise security controls of any computer system unless specifically approved in advance and in writing by the system administrator and with written approval from the Director of Technology Services (TS).
- E. Vendors with access to public networks (Internet, AOL, etc.) must only use their public network user ID in ways that are expressly approved by TS management.
- F. All messages sent using the City's computers, network, or communication devices are the property of the City. E-mail is not private. To properly maintain and manage these systems, management reserves the right to examine all data stored in or transmitted by these systems. Due to the City's computers, network and communication systems being used strictly for business, employees should have no expectation of personal privacy associated with information they store in or send through these City facilities.
- G. Vendors are responsible for ensuring the protection of sensitive information while being printed or viewed on screen.

**CITY OF PLANO POLICIES AND PROCEDURES**

532.000

**Department Name:** Technology Services  
**Procedure:** Vendor and Contractor Network Security Policy

**Effective Date:** 1/1/2005  
**Revision Date(s):** 12/14/2005, 1/18/2006  
**Review: Annual:** 8/1/2006

- H. All systems and computer files that contain confidential information about the City of Plano, its employees, or its customers, shall be maintained on the City's premises and are restricted for authorized use only. This includes information or messages on the email system.

**IV. Password Policy**

- A. Each vendor is responsible for actions taken with his or her network, computer, or logon accounts. To be effective passwords must be complex, changed often, and kept private. Passwords should not be shared.
- B. Poorly chosen passwords can be cracked easily by commonly available password cracking programs. As a result, a poorly chosen password may result in the compromise of the City's network and information. All vendors with access to the City's systems that administrators are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords:
  - 1. All vendors must sign the City's Technology Services Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
  - 2. All passwords must conform to the password construction guidelines described below.
  - 3. All accounts must be uniquely identifiable using the assigned user name. The same password may not be used on more than one account.
  - 4. All vendor passwords must be changed at least every 90 days.
  - 5. Vendor user accounts that have not been accessed within 30 days of creation will be disabled.

**V. GENERAL PASSWORD CONSTRUCTION GUIDELINES**

- A. The passwords you select are the only defense that can prevent someone else from misusing your accounts to improperly access the City network. You are responsible for actions taken using your accounts. Therefore, each individual who is given an account to access any portion of the City's information systems must know how to create a secure password that can not be easily guessed, cracked, or recognized by someone watching over your shoulder.
- B. Passwords must have the following characteristics:

## CITY OF PLANO POLICIES AND PROCEDURES

532.000

**Department Name:** Technology Services  
**Procedure:** Vendor and Contractor Network Security Policy

**Effective Date:** 1/1/2005  
**Revision Date(s):** 12/14/2005, 1/18/2006  
**Review: Annual:** 8/1/2006

1. Contain both upper and lower case characters (e.g., a-z, A-Z)
2. Contain at least one number.
3. Contain a minimum of ten characters (14+ recommended)
4. Not contain single words in any language, slang, dialect, jargon, etc.
5. Not be based on personal information, names of family or pets, anniversary dates, birthdays, etc.
6. Not be characters that appear in sequence on a keyboard, that repeat over and over, or are alphabetically ordered.
7. Contain at least one number and one special character e.g., 0-9, !@#\$%^&\*()\_+|~=-\`{}[]:;'"<>?/,

### VI. Password Protection Standards

- A. Change passwords (e.g. computer, network, application, email, etc.) every 90 days.
- B. Do not use the same password for City accounts as for non-City accounts (e.g., personal ISP account, ATMs, etc.).
- C. Try not to use the same password for your various City login accounts. For example, select one password for your OneWorld login, a separate password for your network login, and another password for your AS/400 login.
- D. Do not share City passwords with coworkers, administrative assistants or secretaries. If any authorized individual has a business need to access information belonging to another user, then Technology Services will give that user the ability to access the needed information using their own login account.
- E. Contact the help desk and ask them to reset your password; if you have to give it to someone for use in an emergency.
- F. Do not write passwords down and store them anywhere they are likely to be found (e.g. desk, keyboard, monitor, wall, a picture, a Post-It-Note, etc.)
- G. Do not use the "Remember Password" feature of applications (e.g., e-mail, web sites, applications, etc.). It is possible for hackers to read saved (remembered) passwords.

**CITY OF PLANO POLICIES AND PROCEDURES**

532.000

**Department Name:** Technology Services  
**Procedure:** Vendor and Contractor Network Security Policy

**Effective Date:** 1/1/2005  
**Revision Date(s):** 12/14/2005, 1/18/2006  
**Review: Annual:** 8/1/2006

- H. Do not insert passwords into email messages or other forms of electronic communications. It is possible for hackers to read passwords in transit.
- I. Do not store passwords in a file on any computer system. The file can usually be read by hackers.
- J. Report a comprised account or password to the Help Desk (972-941-5306) after doing so, change the comprised password.
- K. Configure automatic screensaver locks. The locks should be set to engage after 10 minutes or less of computer inactivity (Individual Departments may have more stringent requirements).
- L. Lock their computer whenever they plan to be away for more than a few minutes to prevent unauthorized use of their user accounts.
- M. Security tests may be performed periodically by Technology Services. Vendors found to have weak passwords will be required to change them.
  - 1. Vendors with accounts that are found to have weak passwords will be required to change their passwords.
  - 2. Violation of this policy may result in a termination of vendor contracts and relations.

**VII. Physical and Manual Security Protection Practices**

Vendors may not connect personally owned PCs or laptop computers to the City's network without prior written approval from the Director of Technology Services.

**VIII. Vendor Access**

The purpose of the City's Vendor and Contractor Access Policy is to establish the rules for vendor access to the City's network and support services. The policy applies to all vendors that are responsible for the installation of new Technology Services assets, and the operations and maintenance of existing resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

- A. Vendors must comply with all applicable City policies, practice standards and agreements. Including but not limited to:
  - 1. Safety Policies

**CITY OF PLANO POLICIES AND PROCEDURES**

532.000

**Department Name:** Technology Services  
**Procedure:** Vendor and Contractor Network Security Policy

**Effective Date:** 1/1/2005  
**Revision Date(s):** 12/14/2005, 1/18/2006  
**Review: Annual:** 8/1/2006

2. Privacy Policies
  3. Security Policies
  4. Auditing Policies
  5. Software Licensing Policies
  6. Acceptable use policy.
- B. Vendor agreements and contracts must specify:
1. The City information the vendor should have access to.
  2. How City information is to be protected by the vendor.
  3. Acceptable methods for return, destruction, or disposal of the City information in the vendor's possession at the end of the contract.
  4. The vendor must only use City information and Technology Services for the purpose of the business agreement.
  5. Any other City information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.
  6. The contracts should all include the form found in the Appendix executed by the vendor.
- C. The City will provide a Technology Services point of contact. This City employee will work with the vendor to insure compliance with the policy.
- D. Vendor must provide the City with a list of employees working on the contract. The list must be updated and provided to the City within 24 hours of staff changes.
- E. On-site vendor employees must acquire and display a City identification badge at all times. Badges will be returned when an employee leaves, or at the end of the contract.
- F. If vendor management is involved in City security incident management the responsibilities and details must be specified in the contract.
- G. Vendor must follow all applicable City change control processes and procedures.

**CITY OF PLANO POLICIES AND PROCEDURES**

532.000

**Department Name:** Technology Services  
**Procedure:** Vendor and Contractor Network Security Policy

**Effective Date:** 1/1/2005  
**Revision Date(s):** 12/14/2005, 1/18/2006  
**Review: Annual:** 8/1/2006

- H. Jeopardizing the city's network intentionally or unintentionally, or violating this policy, will result in revocation of access to City resources.
- I. Regular work hours and duties will be defined in the contract. Exceptions must have prior written approval of the Technical Services Director.
- J. All vendor maintenance equipment and accounts on the City network that connect to the outside world via the network, telephone line, or leased line, will remain disabled, except when in use for authorized maintenance.
- K. Vendor's major work activities must be entered into a log and available to City management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- L. Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to the City or destroyed within 24 hours.
- M. Upon termination of contract or at the request of the City, the vendor will return or destroy all City information and provide written certification of that return or destruction within 24 hours.
- N. Vendors are required to comply with all City auditing requirements, including the auditing of the vendor's work.
- O. All software used by the vendor in providing service to the City must be properly inventoried and licensed.
- P. All vendors will undergo background checks, as required by Federal and State law, prior to being allowed access to the City network and information.

**IX. Appendix**

Vendor Connection Agreement, Dated 03/23/05

## VENDOR CONNECTION AGREEMENT

DATED 03/23/05

This Connection Agreement (the "Agreement") is entered into by and between The City of Plano (the "City"), a municipal corporation and \_\_\_\_\_ Vendor"), a \_\_\_\_\_, on the \_\_\_\_\_ day of \_\_\_\_\_, \_\_\_\_\_, City and Vendor may be referred to herein individually as a "Party" or collectively as the "Parties".

WHEREAS, the City

WHEREAS, the Vendor

NOW THEREFORE, the Parties hereto agree as follows:

### **Technical Requirements. Vendor understands and agrees that:**

The Vendor acknowledges by signing this document that they have read and accept all applicable terms of the City's Security Policy. The City only allows remote access to their network by an authorized virtual private network ("VPN") connection. The City does not allow any Microsoft virtual private network ("VPN") solution for remote access; devices originating a VPN connection must be separated from the public Internet by a hardware/software firewall and must also use a commercially available anti-virus package; local area network ("LAN") devices originating a VPN connection must be addressed from address space allocated in RFC 1918; that Vendor shall be responsible for and shall bear any and all expense for modifications it must make to its configuration or equipment in order to comply with these requirements; and Vendor assumes any and all risk associated with connecting to the City and its network, and the City shall not be responsible for any security breaches on Vendor's network resulting from or related to Vendor's use of the City approved VPN client.

**Limitations on Use.** Vendor understands and agrees that the City may, in its sole discretion, and without advanced notice to Vendor;

1. Assign VPN bandwidth to vendors on an individual basis;
2. Limit the number of concurrent connections that may be made by any Vendor at any one time.
3. Disconnect any vendor responsible for the origination of network traffic that the City deems to be unnecessary, harmful, or disruptive
4. Enforce security policy that requires unique login credentials be supplied for each VPN connection with the understanding that these logon credentials are subject to change every 45 days; and
5. Immediately de-activate VPN accounts upon notification by Vendor of a change in employment status of any employee granted access to the City's network.

**Liability.** Vendor expressly agrees that it shall be liable for any and all damages, including but not limited to actual, consequential, or incidental damages, for disruptions caused by their negligence or intentional misconduct to the City's network, 911 system, or other network services resulting from or related to Vendor's connection to the City's networks. Vendor also expressly agrees to notify the City of staffing changes involving employees with access to the City's network within 24 hours.

Signature\_\_\_\_\_

Name (Printed) \_\_\_\_\_

Title\_\_\_\_\_

Company\_\_\_\_\_

Date: \_\_\_\_\_