ADMINISTRATIVE DIRECTIVE

Title:	Network Access & Security
Issuing Department:	Technology Services
Effective Date:	August 14, 2019
Approved:	Jamsheed Mehta, Town Manager
Type of Action:	Revision

1.0 PURPOSE

Consistent standards for network access and authentication are critical to information security and are often required by regulations or third-party agreements. Any user accessing the Town's computer systems and network has the ability to affect the security of all users of the network. The purpose of this directive is to describe what steps must be taken to ensure that users connecting to the Town network and systems are authenticated in an appropriate manner, in compliance with Town standards, and are given the least amount of access required to perform their job functions. This directive reduces the risk of a security incident by requiring consistent application of authentication and access standards across the network.

2.0 DEPARTMENTS AFFECTED

2.1 This directive applies to:

2.1.1 All Town of Marana departments and employees.

2.1.2 Guests, contractors, and anyone requiring access to the Town network.

2.2 This directive does not govern public access to the Town's externally-reachable systems, such as the Town website or public web applications, or the assignment and use of police video or mobile data terminal equipment.

3.0 REFERENCES

3.1 Town of Marana Personnel Policies and Procedures, Policy 5-4: Use of communications systems and equipment

3.2 Town of Marana Administrative Directive: Electronic Mail (E-mail) Retention & Storage

3.3 Town of Marana Administrative Directive: Mobile Communication Equipment

3.4 Town of Marana Administrative Directive: Staff Network Acceptable Use

4.0 DEFINITIONS

4.1 Account: An established relationship between a user and a network or system.

4.2 Administrative rights: The highest level of permission that is granted to a computer user; this level of permission normally allows the user to install software and change configuration settings.

4.3 Antivirus software: An application used to protect a computer from viruses, typically through real time defenses and periodic scanning; antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

4.4 Authentication: A security method used to verify the identity of a user and authorize access to a system or network.

4.5 Biometric identification: The process of using a person's unique physical characteristics to prove that person's identity; fingerprints, retinal patterns, and hand geometry are commonly used for this purpose.

4.6 Business network or network: Unless the context indicates otherwise, computing network owned and maintained by the Town of Marana for the purposes of conducting Town business including electronic correspondence and data storage, transfer and retrieval.

4.7 Encryption: The process of encoding data with an algorithm so that it is unintelligible without the key; used to protect data during transmission or while stored.

4.8 Non-exempt employees: Employees who devote most of their hours to activities that are not managerial, administrative or professional. These employees are entitled to overtime pay under specific provisions of federal and state laws.

4.9 Password: A sequence of characters that is used to authenticate a user to a file, computer, or network; also known as a passphrase or passcode.

4.10 Virtual Private Network (VPN): A network that uses the internet to transfer information using secure methods.

5.0 POLICIES AND PROCEDURES

5.1 Account Setup. During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

5.1.1 Users will be required to change their password upon first login after account creation.

5.1.2 Users will be granted the least amount of network access required to perform their job functions.

5.1.3 Administrative rights to accounts will not be granted without the approval of the Technology Services Director.

5.2 Account Use. User accounts will be implemented in a standard manner and used consistently across the Town. The following policies apply to account use:

5.2.1 Accounts must be created using a standard format of first initial last name.

5.2.2 Accounts must be password protected.

5.2.3 Accounts must be for individual use only. Account sharing is not permitted.

5.2.4 Accounts must be unique and different from any personal account names.

5.2.5 Occasionally guests will have a legitimate business need for access to the Town business network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, will be restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

5.2.6 All accounts are subject to monitoring or auditing at the discretion of the Town Manager or Technology Services Director, or as required by applicable regulations or third-party agreements.

5.3 Account Suspension and Termination. The Technology Services Director may suspend or terminate an account when the Technology Services Department determines that an account creates a security risk for the Town's network. Accounts will be terminated or suspended when there is a staffing change, including termination or suspension, or a change of job function.

5.4 Authentication. Machines must be configured to request authentication against the network domain at startup. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network.

5.5 Passwords

5.5.1 When accessing the network locally, username and password is an acceptable means of authentication.

5.5.2 Biometric identification can be used in lieu of a user name and password where applicable.

5.5.3 Passwords must be a minimum of eight characters in length.

5.5.4 Employees shall refresh passwords every 90 days.

5.5.5 Employees may not reuse passwords any more frequently than every five password refreshes. For purposes of this paragraph, "reuse" means the use of the exact same password.

5.5.6 Passwords used to access the Town network and systems must be different than those passwords used to access non-Town systems, such as personal banking accounts and personal e-mail accounts.

5.5.7 Employees shall use and store passwords in a secure manner.

5.5.7.1 Employees shall not write passwords down.

5.5.7.2 Passwords must be obscured during entry into information system login screens.

5.5.7.3 Employees shall keep passwords confidential and may not share passwords under any circumstances.

5.5.7.4 Employees shall not send passwords via e-mail or other form of communication, unless they are transmitted in an encrypted format.

5.5.7.5 Employees shall not save passwords in web browsers or applications in order to bypass entering login credentials.

5.6 Remote Network Access. Remote access to the network may be provided to users.

5.6.1 A Department Head may request that employees in certain positions be granted remote network access, based on the duties and responsibilities of the positions and the business need for employees in the positions to have remote network access. The Technology Services Department will grant remote network access when requested by a Department Head, unless the Technology Services Department has determined that there is a security risk in granting the requested access.

5.6.2 For security reasons, access to the Town network will only be allowed via Town-issued equipment and only via an encrypted VPN connection, or similar secure connection, provided by Technology Services.

5.7 Screensaver Passwords. Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. Screensaver passwords are required to be activated after a maximum of 15 minutes of inactivity.

5.8 Minimum Configuration for Access. All devices connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. Technology Services will install and monitor all necessary antivirus and other software to minimize the vulnerability to malicious intent. Devices will not be permitted network access if the necessary software is not installed.

5.9 Encryption. Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the Town network or across a public network such as the internet.

5.10 Logon Failures

5.10.1 Repeated logon failures can indicate an attempt to “crack” a password and surreptitiously access a network account. To guard against password-guessing and brute-force attempts, a user's account will be locked after five unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the Technology Services Director.

5.10.2 To protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

5.11 Town E-mail

5.11.1 Town e-mail shall be used primarily for Town business purposes associated with the performance of each employee's job. Any use of e-mail for non-work related purposes beyond limited incidental use is prohibited.

5.11.2 Town e-mail must not be used for signing up for any websites, online markets, or for access to any sites used for personal purposes

5.11.3 Town e-mail must not be used for creating or forwarding chain letters, Ponzi scams, or other pyramid schemes of any type.

5.11.4 Town e-mail messages and calendars are subject to public records law and Town data retention policy.

5.12 Remote Access to Town E-mail

5.12.1 All employees that have a Town e-mail account may access their e-mail account online through a web browser.

5.12.2 Technology Services will set up e-mail access on personally owned smartphones upon request.

5.12.3 Remote access to e-mail on a smartphone will require that a password or PIN be configured on the phone.

5.12.4 An employee is not entitled to payment of a stipend merely because the employee is granted remote e-mail access through his or her personal mobile communication device. The Town will only pay a stipend pursuant to the policies and procedures described in the Town of Marana Administrative Directive: Mobile Communication Equipment.

5.13 Public Records Law

5.13.1 All records created by an employee’s use of a personal mobile communication device or a personal computer to remotely access the Town’s business network shall be maintained by the Town on the Town’s server in accordance with Arizona law regarding public records and information and Town of Marana Administrative Directive: Electronic Mail (E-mail) Retention & Storage.

5.13.2 Notwithstanding section 5.13.1 above, if an employee uses a personal mobile communication device or a personal computer for Town business, the employee’s personal device or personal computer records may be subject to inspection and/or disclosure pursuant to the public records law or a litigation discovery request. In general, only those portions of the employee’s personal device or personal computer records that are related to Town business should be subject to release or disclosure.

5.14 Fair Labor Standards Act

5.14.1 Time spent by employees remotely accessing the Town network for work purposes, including monitoring, reading and responding to e-mail, is considered compensable time under the federal Fair Labor Standards Act (FLSA) and non-exempt employees must record time spent in these activities as time worked on their time entry for the pay period in question.

5.14.2 Non-exempt employees are prohibited from remotely accessing the Town's network, including their e-mail accounts, by any means during non-working hours, unless the employee is directed to do so by his or her supervisor or any other person authorized to approve overtime work by the employee.

5.14.3 Non-exempt employees who remotely access the Town's network, including their e-mail accounts, by any means during non-working hours without being directed to do so by their supervisor or another authorized person will be subject to disciplinary action pursuant to the Town's Personnel Policies and Procedures.

6.0 RESPONSIBILITIES

6.1 The Technology Services Department will set up remote network and e-mail access for users approved for such access by their departments.

6.2 The Technology Services Department shall maintain a current list of employees granted remote access to the Town's technology network and e-mail.

6.3 Employees who are granted remote network or e-mail access must sign the Technology Services Inventory & Acknowledgment Form (Attachment A) signifying understanding of this directive.

6.4 Employees are responsible for immediately reporting to the Technology Services Department any lost or stolen devices that have Town network access or remote e-mail access configured.

7.0 ATTACHMENTS

7.1 Attachment A - Technology Services Inventory & Acknowledgment Form

Attachment A

Technology Services Inventory & Acknowledgment Form

Employee/Contractor Name: _____ Employee ID: _____

Department: _____Employee/Contractor Position: _____

Date/Update Date/Comments: _____

Reason for Request: ☐ New Hire ☐ New Assignment ☐ Transfer ☐ Lost/Stolen Device ☐ Remote Network Access ☐ Remote E-mail Access

Personal Phone Number (if requesting Stipend): _____

Item	Employee Date Issued/Initials	Manager Date Issued/Initials	Employee Date Return/Initials	Manager Date Return/Initials
Electronic Access ID Card				
Smart or Cell Phone (indicate which)				
Laptop PC				
Tablet				
Stipend (indicate for Smart or Cell Phone)				
Remote Network Access				
Remote E-Mail Access				
Other				

I acknowledge that I have read and understand the Town of Marana Personnel Policies, Procedures and Administrative Directives located on the Town Intranet to include: Policy 5-4: Use of communications systems and equipment; Mobile Communication Equipment AD; Network Access & Security AD; Electronic Mail (Email) Retention & Storage AD; and Facility Access/Keys AD.

I further acknowledge that I have received the above-noted access devices/equipment and that the information contained in the box above is a complete and accurate list of all access devices/equipment currently in my possession.

I further acknowledge that I must return all Town-owned devices/equipment in my possession to my supervisor upon termination of my employment with the Town. I understand that I will be required to replace any missing devices/equipment at my own expense. I understand that if I fail to replace any missing device/equipment, the Town may deduct the value of the unreturned items from my pay. **I authorize the Town of Marana to withhold the value of the unreturned devices/equipment from my final paycheck**. I understand that if the amount from my final paycheck is not sufficient to cover the cost of repayment to the Town, I will be required to reimburse the Town for the amount due at the time of termination.

If I have been granted remote network or e-mail access, I understand that I am not entitled to payment of the stipend established by the Mobile Communication Equipment AD merely because I am granted remote access through my personal mobile device. I understand that the Town will only pay the stipend pursuant to the policies and procedures described in the Mobile Communication Equipment AD. If I am a non-exempt (overtime eligible) employee, I understand that I am not permitted to access the Town network or e-mail systems for work purposes at any time other than their regularly scheduled hours of work without prior approval of my supervisor.

Employee/Contractor Acknowledgment:

Employee/Contractor Signature: _____ Date: _____

If stipend applicable, copy to Finance – Payroll Administrator, Attach the TS Request /Access Form (seamlessdoc)

REVISION HISTORY

	DESCRIPTION OF CHANGE	*DATE*
OR	Original Release	6/1/2018
REV	Revision	8/14/2019

Caution: A copy of this Administrative Directive is an uncontrolled document. It is your responsibility to ensure you are using the current version. The electronic version is the only acceptable and controlled Administrative Directive.