	MANAGEMENT POLICY	POLICY NUMBER: 326
	INFORMATION SECURITY and COMPUTER USAGE POLICY	EFFECTIVE DATE: 03/15/2002 Revised: 06/12/2019

I. PURPOSE

Establish the City of Mesa’s Information Security and Computer Usage Policy to protect the confidentiality, integrity, and availability of the data stored on, redirected through, or processed by, City technology resources.

The term “City technology resource,” includes, but is not limited to, the Internet, Intranet, email, instant messaging, telephones, mobile or [Internet of Things Standard \(IoT\)](#) devices (DVRs, web cameras, TVs, etc.), and other computing and telecommunications resources.

The elements in this policy provide measures that:

- Help preserve the public trust and information;
- Increase City staff’s effectiveness by promoting efficient, clear, and accurate electronic business transactions and communications;
- Minimize security incidents;
- Minimize impact of security incidents and facilitate quick recovery;
- Emphasize the public record aspects of electronic information;
- Protect the City from legal liability;
- Support Payment Card Industry (PCI) obligations;
- Support Health Insurance Portability and Accountability Act (HIPAA) regulations;
- Support FBI CJIS compliance (where applicable);
- Help prioritize criticality and security of City data.

Please note, this Management Policy has been condensed to reflect the City’s intent on how it secures information and is considered appropriate technology use. This document refers to several IT standards that contain detailed information on a variety of topics that fall under Management Policy 326. The Information Technology Department will regularly update these standards so that the City of Mesa keeps abreast of rapidly changing technology, trends, and cybersecurity threats. These standards can be found at ITD’s SharePoint site, which is located under the [‘ITD Policies & Standards’](#) tile.

II. SECURITY POSTURE

The City will use a layered approach of overlapping controls, monitoring, authentication, scanning, and auditing to maintain a high level of information security and privacy among the City’s data, network, and technology resources.

Access to City information systems and data will be granted using the principle of least privilege (need to know). Passwords and credentials used for access to City data and systems, will be strong, individually-owned, changed frequently, and always transmitted and stored encrypted, protected, and never disclosed to anyone. The Information Technology Department will conduct reviews to identify threats and vulnerabilities, which will initiate a formal risk assessment.

III. **SCOPE OF POLICY**

This policy applies to City of Mesa full and part-time employees, contractors, consultants, temporary employees, student assistants, volunteers, vendors, and other users, including those affiliated with third parties who access City of Mesa technology resource(s), all of whom are referred to as “staff” in this policy. This policy applies to all operating systems, computer platforms (mobile and [IoT](#) included), and application systems. Staff is responsible for learning and complying with all City policies, procedures, standards, and local, state, and other laws related to information security. Nothing in this policy supersedes [Mesa’s Personnel Rules](#) related to Section 510 Standards of Conduct.

This policy does not govern physical security. Refer to Management Policy 116 - Identification/Access Cards for physical security.

This policy addresses the retention and disposal of credit card Cardholder Data but does not govern the handling of credit card data. Refer to Management Policy 212 – Credit Card Handling.

IV. **ROLES and RESPONSIBILITIES**

Department Directors, managers, and supervisors:

- Responsible for enforcing this policy and for taking appropriate corrective and/or disciplinary action when a violation of this policy occurs.

Chief Information Officer (CIO), Chief Information Security Officer (CISO) or designee:

- Responsible for interpreting and revising this policy and standards found under the '[ITD Policies & Standards](#)' tile.
- May suspend computing services to staff when deemed necessary.

City Staff:

- Responsible for understanding and complying with this policy and any modifications to the policy;
- Responsible for annually signing an acknowledgment indicating review, understanding, and compliance of the policy.
- Responsible for care, protection and appropriate usage of the City’s technology resources;
- Responsible for changing his/her passwords frequently;
- Protect their passwords and shall never disclose to anyone, including family and other household members when work is being done at home;

- May not use another's user ID and password. Exceptions must be approved by the Chief Information Officer or designee;
- May not connect non-city owned devices to the City's network, except where specific access is granted or services are provided by ITD, or as designated by the standards found under the '[ITD Policies & Standards](#)' tile;
- Immediately report all suspected policy violations, system intrusions, virus infestations, and other conditions that might jeopardize City information or information systems to the Information Technology Help Desk.

ITD:

- May modify this, the standards library, and other IT related policies, to reflect changes in industry standards, legislation, technology, and/or products, services, and processes at the City.
- Will identify threats and vulnerabilities when major changes are made to technology resources.

Non-Employees:

Before being issued a user account, contractors, consultants, student assistants, volunteers, vendors, and other users, including those affiliated with third parties who access City of Mesa technology resources, shall sign an acknowledgement that the individual understands and agrees to comply with this Information Security Policy.

V. POLICY STATEMENTS

1.0 General Use

1.1 City Staff Accountability. City Staff are accountable for the security of their user ID's and passwords, and for all actions performed by their user accounts. This includes using password or other authentication options, as approved by the CIO, CISO or designee, when using a mobile device that accesses City applications or resources, e.g. email. Any activity performed under a staff member's login ID on a mobile device or workstation is presumed to be performed by that staff member and is the responsibility of that staff member.

1.2 Ownership. Technology resources and the data on them are the property of the City and are to be used for City business purposes. Upon termination of City employment, contract, or agreement, personnel must return all equipment, software, and information/data, whether in electronic form or otherwise.

1.3 Privacy Expectations. Staff shall have no expectation of privacy in the use of any City-provided technology resources. Information systems and the data on them are the property of the City and are to be used for City business purposes. All electronic communications sent, received, or stored

on City technology resources are considered City property and may be read at any time. Any City data and electronic communication are subject to the

public records law and may be provided to third parties to comply with this law. Certain exceptions are made for information made confidential by statute or other law, but staff should not consider electronic communication to be private.

- 1.4 Records Management.** City staff must comply with all records retention policies and schedules. City staff responsibilities for records retention of paper documents also apply to electronic documents. Please refer to Policy 105 – Records Management.

City file shares, whether stored on City devices, or in the cloud, shall only contain business-related data and shall not be used to store personal files and/or data.

Email is a method of transit and is not to be used to store public records. Email mail files and archives will be retained for 3 years with automatic deletion of email older than 3 years, performed monthly.

City staff shall follow data classification processes to set retention schedules where available, such as the procedures provided when creating and saving files using such tools as, Office 365 and FileNet document management.

- 1.5 Required Training.** City staff must complete all applicable information security awareness training within City-established timeframes.

- 1.6 System Use.** Technology resources are provided to staff to perform work tasks that support the mission and Charter of the City and shall be used in compliance with Section 510 of the City of Mesa Personnel rules, City of Mesa Code of Ethics, and other related management policies

2.0 System and Network Activities

- 2.1 Authorized Hardware.** It is understood that City staff who access City email via the Internet, or work remotely via the City's remote access system, may use non-City-owned devices for these functions, provided that such devices are regularly updated with the latest security patches and are secured and compliant with anti-virus, and other available security protection measures.

Sensitive information, such as social security numbers, credit card, and protected health information, may be stored on removable media only when necessary, encrypted using only ITD approved encryption methods as approved by the CIO, CISO or designee, and with the knowledge and consent of IT Security. Social security number, credit card number, and

protected health information must be encrypted in transmission, encrypted at rest, and accessible in a secure manner.

Wireless connections, such as wireless access points (WAP's) connected directly to the City's network and other technology resources, must be

approved by ITD and shall comply with identified procedures. Use of network sniffers, scanners, or other network monitoring devices is restricted to Information Technology system administrators who must use such tools to perform their job duties. They will not be used to monitor or track any individual's data activity, except under special authorization approved by the CIO, CISO, and the City Manager, or designee.

- 2.2 Authorized Software.** Employees who install "freeware/shareware" software in support of City business are responsible for obtaining department approval and are accountable for the copyright and licensing requirements and any needed software/system patch and update processes for the software. ITD is available upon request, should departments seek assistance with software review and installation.

For hardware and software that require a purchase, ITD has central oversight and responsibility and may delegate that responsibility to specific areas or departments.

Audits for software compliance may be conducted by ITD and the employee/department will be held responsible for compliance. If a software or hardware is determined by ITD to cause concerns with PC or enterprise performance, the product may be removed by ITD and alternative software sought.

- 2.3 Copyrights and Licensing.** City staff must always comply with all applicable copyright and license requirements.

- 2.4 Personal Use.** While some incidental personal use of City-owned technology resources is acceptable, such incidental use is not a right, and must never interfere with the performance of duties or service to the public. For purposes of this policy, "incidental personal use" is defined as any personal use of City-owned technology resources or managed technology that:

- Is infrequent and brief;
- Does not have a negative impact on overall staff productivity;
- Does not interfere with the normal operations of a staff member's department or work unit;
- Does not result in any additional expense to the City;
- Should not adversely affect technology resources, disk space, and network bandwidth;
- Does not compromise or embarrass either the City or its staff in any way;
- Does not contravene other elements of the Information Security Policy; and/or

- Serves the interests of the City in allowing staff the flexibility to address important personal matters that cannot otherwise be addressed outside of work hours or without leaving the workplace.

Such usage shall not be considered private and is subject to be investigated, monitored, duplicated, recorded, and/or logged.

2.5 Security Software. City staff must not disable or circumvent any software or controls intended to safeguard City technology resources.

City staff must immediately disconnect from any web site they have inadvertently connected to that contains inappropriate content and report the situation to their immediate supervisor. If City staff unintentionally receives inappropriate material, they should report the situation to their immediate supervisor and the Information Technology Help Desk. Information Technology Security personnel can assist in investigating the source of the messages. The inappropriate material shall not be forwarded to other individuals except as instructed by the Help Desk.

The City recognizes that certain departments within the City have a business need to access Internet sites that may be considered inappropriate for others. Filtering tools allow the City to restrict certain types of Internet sites, while allowing exceptions to the restriction. Staff who have a business need to access these Internet sites should obtain written authority from their department director, who will submit the request to ITD Security. All monitoring of access will be done in accordance with City policies, City Personnel rules, state and other applicable laws.

2.6 Unattended Devices. City staff must appropriately protect all unattended technology resources and promptly report any suspicious activity that may affect information security, or the loss or theft of a device containing City information to their immediate supervisor and the Information Technology Help Desk. Staff agrees to follow standard procedures related to password protecting their devices when access to City resources is provided (such as email and other applications). This includes the ability for the City to block use or application access during the loss or theft of City or personally purchased mobile devices that access City applications and resources.

2.7 Inappropriate Use of City Technology Resources. Certain activities constitute an inappropriate use of City technological resources and are expressly prohibited unless an exception is requested by a department director and approved by the CIO or CISO, and the City Attorney, or designee. For more information, and a non-exhaustive list of prohibited activities, see [ITD Security Standard](#).

2.8 Lost Devices. Lost devices pose a significant security and legal risk to the City. For device definitions, the protocols for reporting lost devices, and more information, see ITD's [Mobile Device Standard](#).

- 3.0 HIPAA, PCI, and Data Security Compliance.** The City of Mesa is required to comply with various industry and legal data security requirements. For additional information, the federal standards, and a summary of the federal standards, see ITD's [Compliance Requirements Standard](#).
- 4.0 Data.** Managing the critical data assets of the City is a requirement for all departments. For data definitions, protections, and responsibilities, see [ITD Security Standard](#).
- 5.0 Cloud.** The City is moving more and more of its services out to the cloud, which come with their own set of security concerns. For data definitions, protections, and responsibilities, see ITD's [Cloud Security Standard](#).
- 5.1 CCTV and Web Cameras.** The use of CCTV (close caption television) and web cameras are sensitive devices with specific security concerns. For data definitions, protections, and responsibilities, see ITD's [CCTV and Web Camera Standard](#).

VI. PRIVACY AND WEB/INTERNET GUIDELINES

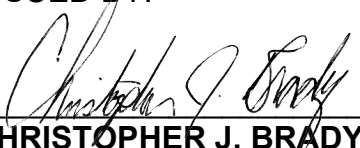
For information about City staff privacy expectations and the use of web resources as communication and service delivery mechanisms, see [ITD Security Standard](#).

VII. COMPLIANCE

Violation of this Management Policy, or any related Information Security Policies, may result in disciplinary actions as authorized by the City in accordance with City policies, procedures, and codes of conduct, up to, and including, termination. Criminal or civil action may be taken if local, state, or other laws are found to have been violated.

The City Auditor may conduct periodic audits to evaluate compliance with the responsibilities set forth in this policy. The City Manager may authorize an outside technology expert to perform audits of City technology resources.

ISSUED BY:



CHRISTOPHER J. BRADY
City Manager

EMPLOYEE ACKNOWLEDGEMENT

Information Security and Computer Usage Policy

I hereby acknowledge receipt of the City of Mesa's Information Security Policy and acknowledge that I understand its contents and agree to comply with its provisions. If applicable, I also acknowledge completing the annual security awareness training requirement (including but not limited to ITD and employees processing credit cards or having access to credit card data). Since the information contained in this policy is subject to change, I understand that it is my responsibility to comply with any revisions to this policy.

Employee's Name (printed)

Employee's Signature

Date: _____

Employee Number: _____

Supervisors: You must complete for any individual who has a user account. Once completed, retain in the individual's workstation file.

NON-EMPLOYEE ACKNOWLEDGEMENT Information Security and Computer Usage Policy

I hereby acknowledge receipt of the City of Mesa's Information Security Policy and acknowledge that I understand its contents and agree to comply with its provisions. If applicable, I also acknowledge completing the annual security awareness training requirement (individuals processing credit cards and/or having access to credit card data). Since the information contained in this policy is subject to change, I understand that it is my responsibility to comply with any revisions to this policy.

Name (printed)

Signature

Date: _____

Badge ID #: _____