mesa·az	MANAGEMENT POLICY	**POLICY NUMBER:** 326
	INFORMATION SECURITY & COMPUTER USAGE POLICY	**EFFECTIVE DATE:** 03/15/2002 Revised: 04/13/16

I. PURPOSE

Establish the City of Mesa’s Information Security 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, e-mail, instant messaging, telephones, mobile devices, and other computing and telecommunications resources.

The elements in this policy provide measures that:

- Help preserve the public trust
- Increase City staff’s effectiveness by promoting efficient, clear, and accurate electronic business transactions and communications
- Minimize security incidents
- Emphasize the public record aspects of electronic information, and
- 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)

This revision supersedes Management Policy #326-Use of Computer Resources

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, 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:

- Responsible for assuring their department complies with this policy

Chief Information Officer (CIO) or designee:

- Responsible for interpreting and revising this policy
- May suspend computing services to staff when deemed necessary.

City Staff:

- Responsible for understanding and complying with this policy
- Expected to comply with any modifications to the policies at the time they are implemented and shall review this policy annually.
- 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.
- 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 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 annually or when major changes are made to technology resources

Full and Part time employees:
The employee shall sign an acknowledgment annually noting the employee understands and agrees to comply with this Information Security Policy.

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 pattern unlock when using a mobile device that accesses city applications or resources. Any activity performed on a mobile device or workstation under a staff member's login ID 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, 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, including City issued or City paid mobile devices**.** 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 in order 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 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 / 2013 and FileNet document management.

1.5 **Required Training.** City staff, if required, must complete all applicable information security awareness training within the timeframes that the City establishes.

1.6 **System Use.** Technology resources are provided to staff to perform work tasks, which 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 that 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 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 network activity except under special authorization approved by the CIO or designee, the HR director, and a City Attorney.

2.2 Authorized Software. Employees who install “freeware/shareware” software in support of City business are responsible for obtaining department approval of said software 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 such software review and installation.

For hardware and software that requires 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 procedure, “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 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 that has a business need to access these Internet sites should obtain written authority from their Department Director who will submit the request to ITD. 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/pattern 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.

In addition to the items noted above, the following activities are prohibited, unless requested by the staff member’s Department Director and approved by a CIO and a Deputy City Attorney.

1. Using, accessing, storing or transmitting pornographic, obscene, sexually explicit, or other inappropriate materials.
2. Using, accessing, or transmitting offensive, threatening, discriminatory, harassing, racial or hate language or images materials.
3. Using or accessing any non-business streaming media.
4. Circumventing user authentication or security of any host, network or account.
5. Interfering with or denying service to any staff member’s computer system (e.g. denial of service attack).
6. Extensive personal use of the City’s technology resources.

7. Attempts to discover another’s password (e.g. decryption) is not permitted, except by authorized IT Security staff.
8. Unauthorized reading, deleting, copying, modifying or printing another staff member’s E-mail.
9. City staff may neither use nor distribute unauthorized software in the course of performing City business.

The following activities are always prohibited:

1. Engaging in any activity that is illegal under local, State or Federal law or which violates City policy.
2. Any personal use that interrupts City business and that keeps a staff member from performing his/her work.
3. Using City technology resources for personal access to auctions (such as e-Bay) or any other activities that result in private gain or profit.
4. Advertising personal items for sale (except in those Intranet areas officially designed for this type of activity).
5. Soliciting or disseminating information and/or data for political, religious, or other non-business uses not authorized by the City.
6. Generating internet bound unsolicited email otherwise known as spam.
7. Aiding in the collection of email addresses for any unauthorized purpose.
8. Creating or forwarding "chain letters", or "Ponzi" or other "pyramid" schemes of any type.
9. Intentionally developing programs designed to harass other staff or infiltrate a City technology resource and/or damage or alter software components.
10. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Mesa.
11. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City of Mesa or the staff member does not have an active license is strictly prohibited.
12. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
13. Making fraudulent offers of products, items, or services originating from any City of Mesa account.
14. Affecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data for which the employee is not an intended recipient or logging into a server or account that the employee is not

expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a staff member's computer session, via any means, locally or via the Internet/Intranet/Extranet.
16. Any other activities that are considered unacceptable use.

3.0 Credit Card Cardholder Data Retention and Disposal

Cardholder Data shall only be used for legitimate City business purposes. Each Department and Division and supporting computer application that accepts payments by credit card, or otherwise processes Cardholder Data, shall follow the approved Credit Card Cardholder data retention and disposal Policy and Procedure. The Policy and Procedure shall incorporate all necessary Payment Card Industry Data Security Standard (PCI DSS) requirements. Only approved Cardholder Data functions shall retain any Cardholder Data.

3.1 Definitions.

- Payment Card Industry Data Security Standard (PCI DSS): the official published set of industry standards and requirements that all credit card processing merchants must comply with, as set forth by the payment card industry Security Standards Council (see https://www.pcisecuritystandards.org/).

- Credit Card Processing System: any electronic system or service used for the completion of credit card transactions, storage of Cardholder Data, or creation of Cardholder Data receipts or reports, for City merchant accounts. This includes any software applications, hardware or other electronic devices, including those provided by third-party vendors that transmit, store or display Cardholder Data.

- Cardholder Data: the information about a cardholder that is collected for the purpose of processing of a credit card transaction. At a minimum, Cardholder Data consists of the full Primary Account Number (PAN), or the PAN plus any of the following: name, expiration date and/or service code. Service code will not be stored.

- Cardholder Data Retention: the identified length of time Cardholder Data is stored and business reasons for such storage.

- Cardholder Data Disposal: the identified criteria for the removal of stored Cardholder Data.

3.2 Procedures. Each Department or Division shall implement procedures to ensure Cardholder Data is only retained for the following reasons:

A. For active recurring payment processing.
B. For the convenience of active customers choosing a stored credit card as part of an interactive payment process, such as on-line payment processing.
C. For processing a refund of recent payments.

Each Department or Division shall implement procedures to ensure the disposal of Cardholder Data for the following reasons:

D. Data stored on an inactive customer with a zero balance shall be disposed.
E. Data stored on inactive recurring credit card agreements shall be disposed.
F. Data stored on credit cards with an expiration date 30 days or more in the past shall be disposed.
G. Data stored as payment transaction history shall be disposed 30 days post event.

4.0 Data Classification

Data is a critical asset of the City. All employees of the City have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the City, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

Responsibility for Data Management - Department’s Ownership of Data
Department Managers are responsible for ensuring that employees understand their responsibilities in managing the type of data their department uses. Information Technology is available to assist departments with questions about the requirements of different data types especially in terms of electronic use but also in best practices related to securing confidential data in paper form.

4.1 Definitions:

Data Custodian
The Data Custodian maintains the protection of data according to the information security classification associated with it by this policy. The Data Custodian role is the responsibility of Information Technology Department.

Data User

The Data User is a person, organization or entity that interacts with data for the purpose of performing an authorized task. A Data User is responsible for using data in a manner that is consistent with the purpose intended and in compliance with the policy.

Data users shall follow data classification processes where available such as the procedures provided when creating and saving files using such tools as Office 365 / 2013 and FileNet document management.

Data Classification Categories

Data owned, used, created or maintained by the City is classified into the following three categories:

- Public
- Official Use Only
- Confidential

4.2 Data Classification.

A. Public Data

Public data is information that is generally open for public inspection. It is defined as information with few restrictions with existing local, national or international legal restrictions on access or usage. Public data, while subject to the Arizona Public Records Law, is available to all employees and to all individuals and entities external to the City. By way of illustration only, some examples of Public Data include:

- Published press releases
- Department information and services as published on the City's websites
- Published interactive City maps, newsletters, and ordinances

B. Official Use Only Data

Official Use Only Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to employees of the City who have a legitimate purpose for accessing such data. By way of illustration only, some examples of Official Use Data may include:

- Employment data, claims and health information that is not classified as Confidential Data.

- City vendor or partner information where no restrictive confidentiality agreement exists
- Personally identifiable information collected from the public in order for the City to provide services to that individual that is not classified as Confidential Data.

Official Use Only data:

- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
- Paper must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- Should not be stored in personal or shared cloud storage offerings except as approved by the CIO or provided by Information Technology through approved solutions.
- Must not be posted on any public website.
- Must be destroyed when no longer needed subject to the City's Records Management Policy. Destruction may be accomplished by:
  - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
  - Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with the City's IT Security Policy

C. Confidential Data

Confidential Data is information protected by statutes, regulations, City policies or contractual language. Managers may also designate data as confidential subject to and consistent with Arizona Public Records Law. Confidential Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside the City should be authorized by executive management and/or the City Attorney's office.

By way of illustration only, some examples of Confidential Data may include:

- Medical records or any subpart of medical record information
- Social Security Numbers
- Personnel and/or payroll records
- Bank account numbers, credit card numbers and other personal financial information

- Privileged attorney-client communications
- Driver’s License Numbers
- Network, Utility infrastructure diagrams
- Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.

Confidential data:

- When stored in an electronic format, must be protected with strong passwords and stored on servers that have protection and encryption measures provided by the Information Technology Department in order to protect against loss, theft, unauthorized access and unauthorized disclosure.
- Should not be stored in personal or shared cloud storage except as approved by the CIO (or Police Chief for CJIS data) which has been vetted and secured in approved locations certified to hold the type of data in question. For example, the City may require a payment card industry certified service, or in a cloud provider certified and secured to house health information (HIPAA) data or criminal justice (CJIS) certified cloud storage.
- Must not be disclosed to parties without legal authorization.
- Hard copies must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on any public website.
- Must be destroyed when no longer needed subject to the City’s Records Management Policy. Destruction may be accomplished by:
  - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
  - Electronic storage media shall be sanitized appropriately by degaussing prior to disposal or reallocation. Disposal or reallocation of electronic equipment must be performed in accordance with the City’s IT Security Policy.

D. Loss or Unauthorized Disclosure of Confidential Data

The CIO must be notified in a timely manner if data classified as confidential is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the City's information systems has or is suspected of taking place.

5.0 HIPAA Requirements

Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of electronic protected health information (EPHI) within departments where such information is accessed, handled, or stored.

Access to electronic protected health information is to be granted only within the bounds of the "minimum necessary" requirements as defined under HIPAA and to members of the workforce whose job functions are authorized to access such information.

Business Associate contractual agreements must be established with third party entities that fall outside the definition of a "Covered Entity" under HIPAA, when the third party and members of its workforce will have access to or potentially come in contact with electronic protected health information maintained by the City.

VI. PRIVACY

The City reserves the right to investigate, monitor, duplicate, record and/or log all staff use of City technology resources with or without notice to support operational, maintenance, auditing, security, and investigative activities, including enforcement of this policy, legal requests, public record requests, and to help assure and to verify compliance, confidentiality, integrity, and availability of City owned technology resources.

This policy does not prohibit technical staff from monitoring departmental workstations and servers for the purpose of maintaining overall system reliability, availability, and security. This also includes but is not limited to keystrokes, file access, logins, and/or changes to access levels.

Unauthorized accessing, monitoring, or reading of technology resources or their contents violates this City policy. Staff that has elevated privileges shall only use such privileges in the performance of their duties and shall not use such privileges to access systems, applications, information and/or data that would otherwise be inaccessible and shall not access another staff member's accounts, data and/or information without first obtaining approval.

The City Manager and Department Director's may approve initiating an investigation of their staff's compliance with this policy as outlined in the Security Investigation Procedure.

VII. WEB GUIDELINES

The City of Mesa's external (internet) and internal (intranet) web sites are key communication and service delivery mechanisms for employees, residents, businesses and visitors. These sites represent the City of Mesa as well as other interactive Internet applications where the content and presence is in an official City of Mesa capacity.

- Those publishing content, or providing services on the City's or other Internet sites on behalf of the City, will follow all processes, guidelines as and policies established.
- All City of Mesa external and internal web sites will be hosted internally by the City unless exceptions are granted by City Management. New web sites must be approved by the Office of Public Information and Communication prior to being created.
- Additional web addresses (domains) will be requested through the Office of Public Information and Communication and then purchased and maintained by the Information Technology Department.

Use of online interactive tools and social media can be found in Management Policy 359 - Social Media.

VIII. 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

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 (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 #: ____________