City of Meridian
Standard Operating Policy
Number 10.1

Disposal of Media

Purpose:
To set forth the City's policy regarding disposal of media.

Policy:
The City of Meridian recognizes proper disposal of media is necessary to protect sensitive and confidential information, employees and City. Inappropriate disposal of media may put employees and the City at risk. The City has developed proper disposal of media procedures which anyone subject to this policy is required to adhere to.

This policy applies to employees, contractors, temporary staff, and other workers at the City, including all personnel with access to sensitive and confidential data and media. This policy applies to all equipment that processes confidential and sensitive data that is owned or leased by the City.

This policy shall be implemented pursuant to the Disposal of Media Standard Operating Procedures.

Authority & Responsibility:
IT shall be responsible for administering this policy.

City of Meridian
Standard Operating Policy
Number 10.2

Equipment Checkout

Purpose:
To set forth the City's policy for Equipment Checkout.

Policy:
The IT Department is authorized by the City to maintain a pool of equipment for checkout and use by other departments in order to allow for efficient, cost effective operations and services.

This policy shall be implemented pursuit to the Equipment Checkout Standard Operating Procedures.

Authority & Responsibility:
IT shall be responsible for administering this policy.

City of Meridian
Standard Operating Policy
Number 10.3

Identity and Access Management

Purpose:
To set forth the City's policy on required access control measures to all digital identities in use for City information systems to protect the confidentiality, integrity, and availability of City resources.

Policy:
The City follows a standard framework for Identity Management, Authentication, and Access Control. Employees are required to use digital identities to access City information systems, use these identities for authentication, and to do so, only as authorized.

This policy shall be implemented pursuant to the Identity and Access Management Standard Operating Procedures.

Authority & Responsibility:
The Information Technology department is responsible for administering this policy.

City of Meridian
Standard Operating Policy
Number 10.4

Incident Response

Purpose:
To set forth the City's policy regarding Information Technology (IT) Incident Response processes created to protect the City of Meridian's information systems.

Policy:
To protect the City of Meridian's information systems processes are in place to identify and respond to suspected or known incidents that may impact or threaten the integrity of the information systems. Processes include required communication, response, mitigation, and remediation of IT related incidents. Employees, contractors, or others shall report incidents to the IT Department. The IT Department shall report incidents to applicable parties as needed depending on the type of incident and impact.

This policy shall be implemented pursuant to the Incident Response Standard Operating Procedures.

Authority & Responsibility:
IT shall be responsible for administering this policy.

City of Meridian
Standard Operating Policy
Number 10.5

Information Security

Purpose:
To set forth the City's policy regarding information security.

Policy:
The City shall act in due diligence to protect the integrity of the City's information systems, to mitigate the risks and losses associated with security threats to computing resources and to ensure secure and reliable network access and performance. This applies to all City information systems.

This policy shall be implemented pursuant to the Information Security Standard Operating Procedures.

Authority & Responsibility:
IT shall be responsible for administering this policy.

City of Meridian
Standard Operating Policy
Number 10.6

Password Requirements

Purpose:
To set forth the City's policy regarding employee password requirements.

Policy:
The City has a sizeable investment in its information systems that support the City's operations and services. Safeguarding its information systems and the information contained therein is of paramount importance. Password requirements are part of the City's defenses against cyber-attacks. Employees are required to keep passwords confidential, current and compliant with City requirements.

This policy shall be implemented pursuant to the Password Requirements Standard Operating Procedures.

Authority & Responsibility:
IT shall be responsible for administering this policy.

City of Meridian
Standard Operating Policy
Number 10.7

Security Awareness Training

Purpose:
To set forth the City's policy regarding the Security Awareness Training Program.

Policy:
The City has developed an employee Security Awareness Training Program as part of its ongoing efforts to protect the City's Information Systems from security threats and breaches. Lacking adequate information security awareness, staff is less likely to recognize or react appropriately to information security threats and incidents and are more likely to place information assets at risk of compromise. In order to protect information assets, all workers must be informed about relevant, current information security matters. This policy applies to all City employees, contractors, or others, with access to City systems.

This policy shall be implemented pursuant to the Security Awareness Training Standard Operating Procedures.

Authority & Responsibility:
The Chief Information Officer (CIO) or designee shall be responsible for administering this policy.

The CIO is accountable for running an effective security awareness training program that informs and motivates employees to help protect the City's Information Systems and customer information assets.

City of Meridian
Standard Operating Policy
Number 10.8

Technology Purchase

Purpose:
To set forth the City's policy regarding technology purchases.

Policy:
This policy applies to all City technology purchases including hardware and software.

Technology purchases except the accessories listed below must go through the Information Technology (IT) department and conform to IT Standards. Certain technology such as software shall go through an evaluation process.

The IT department manages all hardware and software purchases for the City, including maintenance and support renewals. This service allows us to:

- Reduce department overhead
- Avoid duplicating solutions and efforts
- Adhere to standards when possible
- Renew items on time
- Track hardware and software
- Ensure support and compatibility
- Increase ease and timeliness of support
- Reduce costs
- Avoid extra fees
- Maintain compliance with licensing and subscription agreements

This policy shall be implemented pursuant to the Technology Purchase Standard Operating Procedures.

Authority & Responsibility:
IT shall be responsible for administering this policy.

City of Meridian
Standard Operating Policy
Number 10.9

Technology Replacement

Purpose:
To set forth the City's policy regarding technology replacements.

Policy:
The City shall follow a standard replacement schedule for technology to ensure that computing resources are up-to-date and continue to fulfill operational needs of the City.

This policy shall be implemented pursuant to the Technology Replacement Standard Operating Procedures.

Authority & Responsibility:
IT shall be responsible for administering this policy.

City of Meridian
Standard Operating Procedure
Number 10.1

Disposal of Media

Purpose:
To set forth the City's procedures regarding disposal of media.

Procedures and Related Information:
When no longer usable, storage devices such as USB drives, flash media, hard drives, discs, storage media in cell phones, copiers or other devices, and other similar items used to process or store confidential and/or sensitive data shall be properly disposed of in accordance with measures established by the City. Information systems that have processed, stored, or transmitted sensitive and/or confidential information shall not be released from control until the equipment is sanitized and all stored information has been cleared. The following procedures will be followed.

I. City will dispose of hardware by one of the following methods

   A. Overwriting - an effective method of clearing data from media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located. A minimum of three times is required for sensitive or confidential information.

   B. Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media. This only applies to magnetic media.

   C. Destruction - a method of destroying media. As the name implies, destruction of media is to physically dismantle by methods of crushing, disassembling, etc.

   D. Factory defaults – restoring to factory defaults. (Only applicable to limited feature operating systems such as those that run on cell phones).

II. Enforcement

   A. Any employee found to have violated these procedures may be subject to disciplinary action, up to and including termination of employment.

   B. Supervisors shall report any employee found to have violated these procedures to the IT Director.

   C. The IT Director shall consult with Human Resources to discuss appropriate discipline if warranted.

City of Meridian
Standard Operating Procedure
Number 10.2

Equipment Checkout

Purpose:
To set forth the City's procedures for checking out equipment from the IT Department.

Procedures and Related Information:

I. City employees may check out equipment by submitting a ticket. Equipment will be loaned out on a first-come first-served basis.

   A. Types of available equipment for employee checkout are listed below

      1. Laptops
      2. Projectors
      3. Conference Phone
      4. Video Conference System
      5. Webcams
      6. Hotspots
      7. Cables
      8. Training laptops are not available for checkout

II. Return of Checked Out Equipment

   A. Employees shall return equipment by the date designated by the IT Department.

   B. Employees shall notify the IT Department of any issues, loss or damage related to the checked out equipment as soon as possible, but no later than the return date.

   C. Employees may be liable for loss or damage caused to checked out equipment as determined by the IT Director. The IT Director may consult with the employee's supervisor and Human Resources if deemed necessary.

City of Meridian
Standard Operating Procedure
Number 10.3

Identity and Access Management

Purpose:
To set forth the City's procedures regarding identity and access management.

Procedures and Related Information:

I. Identity

A. Accounts

1. User Accounts: This is a uniquely associated identity for a specific employee. These are the most common type of accounts and are issued to all City employees, contractors, or others. User accounts or passwords shall not be shared with others.

2. Shared Account: These are used to support multiple users sharing the same identity. The use of shared accounts is discouraged as it lacks accountability and security. They shall receive limited access. They are only for specific use cases where there is a business need that cannot be met with standard user account.

3. Service Accounts: A service account is used when it is necessary for systems or applications to authenticate to other systems or applications without any association to a person. Users shall not log in with these accounts.

4. Privileged Accounts: Certain accounts may have extra privileges related to the management of a device or application. This is often thought of as an account type, but it is more accurately described as an account with privileged authorizations. Privileged accounts are granted approval to defined Information Technology (IT) staff. Privileged accounts may be given to employees and contractors as deemed necessary by IT staff.

5. Accounts will expire after 90 days of inactivity unless otherwise noted.

B. New User Accounts

1. Upon notification from the Human Resources (HR) Department, a user account will be created for all new employees. Passwords for new accounts will be provided directly to HR and the employee's supervisor. The initial password provided will be temporary and must be changed once the employee logs into the network.

2. Request for employee access to applications or resources beyond those provided to all employees must be submitted by the employee's supervisor using the ticketing system. Access will be granted based on the resource owner's approval.

C. Removal of User Accounts

1. When an employee separates from the City, supervisors shall give IT notice to ensure that resources are no longer available when the employee leaves.

2. Employee accounts will remain in a "disabled" state for a maximum of 30 days, at which point the account will be deleted from the system. It is the responsibility of the employee's supervisor to notify IT of any resources which may be required of the terminated employee.

II. Authentication

A. The City's standard authentication method is username and password. Some resources require additional authentication known as multifactor authentication.

B. Multifactor Authentication (MFA)

1. MFA involves combining more than one authentication type and generally provides a stronger assurance of the person's identity. MFA is typically utilized in systems involving sensitive, privileged, externally accessible, or cloud applications.

2. MFA shall be used when an information system being accessed contains sensitive or confidential information or when using a privileged account remotely. MFA is recommended in all cloud applications.

C. Directory Services

1. Whenever possible and reasonable, any application or system, whether on premise or in the cloud, should use directory services and single sign on for authentication over local accounts and passwords.

D. Session Lock

1. The City's default session lock value is 15 minutes for all City computers. The IT department may make exceptions to this on a case by case basis.

E. Remote Access

1. Remote access that the city offers includes Virtual Private Network (VPN) services, cloud services, and any other externally accessible system.

2. All remote access services shall be encrypted, authorized, and are subject to expiration of 90 days.

3. A User account is required. Users cannot use a shared account for remote access.

4. MFA shall be required for VPN access and is recommended for other services.

III. Authorization

A. All accounts shall only be used for authorized purposes.

B. Least Privilege

1. An authorization should only provide the privileges required for the function or task to be performed and no more.

C. Separation of Duties

1. Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or security concerns.

IV. Auditing and Accounting

A. The City shall maintain an audit trail of actions performed by identities and shall be reviewed for proper use.

City of Meridian
Standard Operating Procedure
Number 10.4

Incident Response

Purpose:
To set forth the City's procedures regarding communication, response, mitigation, and remediation of Information Technology ("IT") related incidents that impact or threaten the City of Meridian's information systems.

Procedures and Related Information:

I. Scope

A. These procedures apply to all City of Meridian employees, contractors, or others, who process, store, transmit or have access to City of Meridian information systems.

II. Definitions

A. Systems: A software or hardware communications and/or computer-related equipment or interconnected system or subsystems of equipment that is used in the processing, transmission, containment, manipulation, monitoring, management, display or reception of data.

B. Incident: An event that threatens the security, integrity, confidentiality, or availability of a City of Meridian IT related systems or services.

III. Incident Reporting

A. Any City employee, contractor, or others using City equipment is required to report any security incident, suspicious activity or related concern to IT. This includes, but is not limited to, contacting the Helpdesk or other IT employees directly, creating a ticket in the support system, sending an email, and/or contacting the IT After Hours emergency number. IT personnel will ensure that the incident is routed to the appropriate person.

B. Employees, contractors, or others are required to notify IT of theft or a compromised device, even if the theft or the device is personal equipment when connected to a City system (such as email)

IV. Prioritization

A. Incidents will be prioritized by impact (Public web server as opposed to user workstation), and risk (data exposure or destruction).

V. Escalation

A. For incidents of a significant nature, the Chief Information Officer (CIO) or designee is notified and responsible for determining the impact/risk of the incident and notifying and briefing the applicable parties on the incident.

VI. Mitigation and Containment

A. Information Technology employees that receive notification of an incident shall take appropriate action to terminate the activity. Affected systems of the incident will be isolated. A damage assessment will be conducted on the affected equipment or system. Any discovered vulnerability will be repaired as soon as possible.

VII. Eradication and Restoration

A. The damage assessment determines the course of action required to provide a permanent solution. Any repairs, upgrades, and/or data restorations will be conducted urgently, with IT's best effort to meet Recovery Time and Point Objectives (RTOs and RPOs) determined by the department(s) affected by the incident.

VIII. Information Dissemination

A. Any public release of information to the press and/or public regarding an IT related security incident shall be authorized and coordinated through the CIO and the City Communications Manager.

B. The CIO or designee shall manage the dissemination of incident information to other agencies, departments, or personnel. Dissemination to said parties will be based on the impact and risk associated with the incident. Incident reports, including oral discussion, will be given within 24 hours of the incident. Agencies or departments with data of a sensitive nature shall be notified in accordance with their Federal regulation. Any security breach incidents involving PII (Personally Identifiable Information) or CJI (Criminal Justice Information) shall be reported to the Meridian Police Dept Terminal Agency Coordinator ("TAC"), City of Boise, Ada County Sheriff Office, and Idaho State Police. Local law enforcement shall be notified if applicable. See the latest revision of the CJIS Security Policy for more information on CJI/PII.

IX. Ongoing Reporting

A. After initial report of an issue, if not already done, a ticket will be created in City support system in regards to the effect of the incident. If it's determined to be of a significant nature, subsequent reports will be provided to the CIO, IT designee, and others as applicable. Minor incidents will be managed within the IT Department. Updates and resolution notes will be attached to the ticket.

B. An Incident report will contain, but may not be limited to the following items:

1. Point of contact

2. Affected system and physical location(s)
3. System description and application
4. Type of information contained in the system
5. Incident description
6. Incident resolution status
7. Damage assessment, including data loss or corruption
8. Agencies and/or departments contacted
9. Corrective actions taken
10. Knowledge gained/future mitigation

X. Review

A. Analysis of the impact will be ongoing, and a best effort used to implement the resolution on all systems, affected or not, if applicable. Ongoing reports will be given at an appropriate frequency or as requested by the CIO or designee, Mayor, or City Officials.

XI. Training

A. Initial training will be provided during the onboarding process. In addition, Users will receive training at least annually through the security awareness training program.

City of Meridian
Standard Operating Procedure
Number 10.5

Information Security

Purpose:
To set forth the City's procedures regarding information security.

Procedures and Related Information:

I. Network Connections

A. City employees may not connect, nor contract with an outside vendor to connect, any device or system to the City's networks without the prior review and approval of IT.

B. Unauthorized access to City network/server equipment (firewalls, routers, switches, etc.) is prohibited.

C. Unauthorized access to City equipment/cabling rooms/datacenters is also prohibited.

II. Network Security

A. All devices connecting to the network must have adequate security installed and maintained to prohibit unauthorized access or misuse.

B. City reserves the right to quarantine or disconnect any system or device from the City network at any time.

C. City reserves the right to decrypt encrypted traffic.

III. Data Protection

A. Systems hosting City information must be protected in alignment with Information Technology standards and industry best practices. Specifically, systems shall operate with:

1. Physical protection (mobile)
2. Up to date Anti-Virus software
3. A Firewall
4. Software updates applied regularly

IV. Enforcement

A. Attempting to circumvent security or administrative access controls for information systems is a violation of these procedures and will be subject to disciplinary actions up to and including termination.

B. Disciplinary action will be determined by the Chief Information Officer in conjunction with the Human Resources Director and the department director of the violating employee.

V. Monitoring and Auditing

A. City will maintain and monitor logs for all network devices and systems for security auditing purposes.

B. City may perform security audits of any system or device attached to the City network.

City of Meridian
Standard Operating Procedure
Number 10.6

Password Requirements

Purpose:
To set forth the City's procedures regarding password requirements.

Procedures and Related Information:

I. Passwords shall meet the standards in either the basic password standards or advanced password standards as outlined below.

A. Basic Passwords Standards:

1. Expires every 90 days
2. Minimum of 8 characters
3. Must contain 3 of 4 character sets: lowercase, uppercase, number, special character
4. Cannot be the same as username
5. Cannot contain dictionary words
6. Cannot contain proper names
7. Cannot contain compromised passwords
8. Cannot contain more than 3 repeating or sequential characters ("aaaa", "1234", "qwerty")
9. Cannot be identical to the previous 10 passwords
10. Cannot be changed more than once per day

B. Advanced Passwords Standards (Pass phrases):

1. Expires every 365 days
2. Minimum of 20 characters
3. Cannot be the same as username
4. Cannot contain compromised passwords
5. Cannot contain more than 3 repeating or sequential characters ("aaaa", "1234", "qwerty")
6. Cannot be identical to the previous 10 passwords
7. Cannot be changed more than once per day
8. No complexity requirements such as upper / lower case, numbers, symbols. Spaces count as characters

II. Unsuccessful Login Attempts:

A. Account lockout duration: 10 minutes

B. Account lockout threshold: 5 invalid attempts

C. Reset account lock counter after: 10 minutes

III. Employees shall keep all passwords confidential, current and compliant with these procedures. Failure to comply may be grounds for disciplinary action, up to and including termination.

A. Employees shall inform the IT department immediately upon learning of any problem related to the confidentiality or integrity of their password.

B. IT shall provide the necessary support to protect the City's information systems from cyber-attack related to an employee password compromise.

IV. Additional information

A. The City's password program is enforced by Group Policy, Active Directory and Password Policy Enforcer systems that run on City servers and integrate with Microsoft Azure Active Directory.

B. Refer to the following resources for more information on password standards the City adheres to:

1. The National Institute of Science and Technology (NIST) Special Publication 600-83B.

2. The Criminal Justice Information Services (CJIS) Security Policy.

City of Meridian
Standard Operating Procedure
Number 10.7

Security Awareness Training

Purpose:
To set forth the City's procedures regarding security awareness training.

Procedures and Related Information:

I. Security Awareness Training

A. The City Information Technology ("IT") department requires that each employee upon hire and at least annually thereafter successfully complete security awareness training. Certain staff may be required to complete additional training depending on their specific job requirements. Staff will be given a reasonable amount time to complete each course to not disrupt business operations. IT will also provide security awareness information which is to be reviewed by employees. (Emails / video monthly except when we do online training).

II. Simulated Social Engineering Exercises

A. The 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 IT department will conduct these tests at random throughout the year with no set schedule or frequency. The City IT department may conduct targeted exercises against specific departments or individuals based on a risk determination.

III. Remedial Training Exercises

A. From time to time City employees may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the IT department as part of a risk-based assessment.

IV. Compliance & Non-Compliance

A. Compliance with these procedures is mandatory for all employees, contractors, elected officials and others. Violation of these procedures by employees may be cause for disciplinary actions up to and including termination. The CIO in conjunction with the Human Resources Director and the department director of the employee will address violations and determine the appropriate discipline as needed.

B. All supervisors are responsible for ensuring that their staff and other workers within their responsibility participate in the security awareness training, and educational activities where appropriate and required.

C. The IT department will monitor compliance and non-compliance with these procedures and report the results of training and social engineering exercises to the leadership team.

V. Compliance Actions

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

B. A "Pass" includes but is not limited to:
   1. Successfully identifying a simulated social engineering exercise
   2. Not having a Failure during a social engineering exercise (Non-action)
   3. Reporting real social engineering attacks to the IT department

VI. Non-Compliance Actions

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

B. “Failure” includes but is not limited to:
   1. Failure to complete required training within the time allotted
   2. Failure of a social engineering exercise
   3. Failure of a social engineering attack

C. Additional actions not outlined in these procedures may be required in the event of a failure associated with an actual social engineering attack, commensurate with the risk and / or damages to the City.

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

   1. Clicking on a URL within a phishing test
   2. Replying with any information to a phishing test
   3. Opening an attachment that is part of a phishing test
   4. Enabling macros that are within an attachment as part of a phishing test
   5. Allowing exploit code to run as part of a phishing test
   6. Entering any data within a landing page as part of a phishing test
   7. Transmitting any information as part of a vishing test
   8. Replying with any information to a smishing test
   9. Plugging in a USB stick or removable drive as part of a social engineering exercise
   10. Failing to follow City procedures during a physical social engineering exercise

E. The IT department may also determine, on a case by case basis, that specific failures are a false positive and should be removed from that staff member's total failure count.

VII. Failure Penalties

A. The following outlines the penalty of non-compliance with these procedures. Steps not listed here may be taken by the IT department to reduce the risk that an individual may pose to the City.

B. Social Engineering

1. First Failure - Notification from IT providing feedback on incorrect action. (Occurs on all phishing failures)
2. Second Failure – Mandatory completion of remedial training and discussion with supervisor. (Documented)
3. Third Failure – Training with IT, which is documented. This and subsequent failures may be subject to disciplinary action, up to and including termination.

C. Training

1. First Failure – Notification from IT and supervisor to take correction action.
2. Second Failure – Discussion with supervisor. Computer access revoked until corrective action is take. (User account disabled)
3. This and subsequent failures may be subject to disciplinary action, up to and including termination.

VIII. Record Keeping

A. Records of all Compliance and Non-Compliance Actions shall be kept by the IT department for a rolling eighteen (18) month period. Any actions older than 18 months will not be considered for failure penalties.

City of Meridian
Standard Operating Procedure
Number 10.8

Technology Purchases

Purpose:
To set forth the City's procedures for technology purchases.

Procedures and Related Information:
Technology purchases shall meet the standards as outlined below.

I. Technology Purchases

A. The following items must be purchased through IT. Requests can be made through the IT Ticketing System:

1. Software
2. Software as a service (SaaS) - any software that's licensed on a subscription basis and is hosted outside the City network
3. Website / Hosting Services / Software Development
4. Computers (including Desktops, Workstations, Laptops, MDTs, Tablets, iPads)
5. Monitors
6. Printers / Copiers / Scanners
7. Phones (Mitel) – including Bluetooth Headsets
8. Conference / Video Conference Solutions
9. Network / Server Equipment
10. Mobile Apps for City Use
11. Any accessories or peripherals not listed below
12. Maintenance / support renewals, subscriptions, etc. of aforementioned items

B. Accessories listed below can be ordered by departments without having to request them through IT:

1. Mouse
2. Keyboard
3. Flash Drive
4. Digital Camera
5. Computer Speakers
6. Bluetooth Headsets for Cell Phones
7. iPad Case
8. HDMI or USB cables
9. Headphones for computers (wired recommended)

C. IT has the following items on hand (but the department will still be charged):

1. Mouse
2. Keyboards
3. Monitors
4. Desk Phones
5. Computer Speakers

II. Software Evaluation

A. This defines the software evaluation process required to purchase software. This policy does not apply to upgrades of existing software. That is, software which the city currently owns, and the vendor of said software, is merely adding additional features or functionality in a newer version (i.e. version 6.1 to 7.0).

1. Department Directors (or designee) shall contact IT prior to beginning any software project.
2. The software evaluation process should be commensurate to the cost of the existing software the City owns and the cost of the new software.
3. IT will evaluate any new software system against existing software the City owns to maintain consistency and standards. The following questions will be used in the evaluation process.

B. Questions for Department

1. What are the requirements? (What are the business needs?)
2. What is currently being used to fill these needs?
3. Is the software budgeted for?
4. What is the cost? (one time & recurring)
5. Is the software on premise or cloud based?
6. What is the implementation timeframe?
7. Who is providing training?
8. Are there plans to integrate it with other systems?
9. Will users access the system remotely? If so, how?
10. Will it require custom reporting? Will the vendor create the custom reports? If so, how many are included in the quote for install?
11. Will end users configure additional needed reports in the future or will IT need to allocate resources for this function?
12. How many users will be using the system? (How many installations will be needed?)
13. What is the plan for migrating any existing data into the system?
14. Are there any security or encryption requirements?
15. What is the retention for the data storage? How will records retention be managed for the software?

C. Questions for Vendor

1. General for Both (SaaS & On-Prem)

    a. Will users be able to run it without administrative privileges?
    b. What is the minimum resolution supported? (800x600, 1024x768, etc..)
    c. Is there support for Single Sign On (SSO)? (SAML, AD integration, etc)
    d. What are the minimum hardware requirements? (CPU, HD, RAM)
    e. How is licensing set up? (Per user, device, concurrent, site wide, etc)
    f. Is there recurring maintenance, support, or subscription costs?

2. On Premise

    a. Can you provide a system architecture diagram?
    b. What is the database type? (SQL Server, Oracle, MySQL, etc) What versions are supported?
    c. Is it compatible with Windows Server 2016 for server-side and Windows 10 for client-side?
    d. Is it delivered over a web browser or client-server? If web, what browsers are supported? If web based, does it use responsive web design?
    e. What web server/container does it run on? (IIS, Apache)
    f. Who does the installation and subsequent maintenance?
    g. Is SSRS supported for reporting?
    h. What type of runtime will it operate in? (.NET, VB 6 Runtime, Java, Windows Runtime, Windows Universal Runtime, Win32, Silverlight, Flash, etc)
    i. Will any portion of the software be accessible from the internet?

3. Hosted/Software as a Service (SaaS)

    a. What platform is it hosted on? (AWS, Azure, Private datacenter, etc)
    b. Can we gain access to the data for reporting or integration needs?
    c. Are there any additional components that we will need to install? (ActiveX, Java, Flash, etc.)
    d. Can we get a copy of the data if we part ways with the product? What format will it be in? Can we get a copy of the data regularly for other needs?
    e. Is it delivered over a web browser or client-server? If web based, what browsers are supported? If web based, does it use responsive web design?
    f. Do you have any API's for integration? Is there an additional cost to them?
    g. What are the data protection services offered? (Backup, redundancy, frequency)

City of Meridian
Standard Operating Procedure
Number 10.9

Technology Replacement

Purpose:
To set forth the City's procedures for replacing technology.

Procedures and Related Information:

I. The following schedule is used to replace hardware and software. All equipment will be replaced on this schedule. However, if a particular lot of equipment is problematic it may be necessary to replace equipment outside of the normal replacement cycle.

A.	Infrastructure:	4 years or as needed
B.	Computers:	5 years or as needed
C.	Software:	6 years or as needed
D.	Printers:	7 years or as needed

II. Replaced equipment will be disposed following the City's Asset Disposal policy. Once equipment has been funded for replacement, this equipment is not eligible to be included as a replacement request (G200) a second time.