IT Best Practices for small municipalities

Executive Summary

Small municipalities frequently rely on Information Technology (IT) to maintain day to day operations however the understanding of the resources, information, maintenance and associated costs of IT are often overwhelming for town administration. This document and associated checklists serve as a guide to aid in familiarization, evaluation, and planning with recommendations of best practices. It includes information to introduce key concepts and prerequisites to enable the decision-making process while not being an Information Technology specialist. Introduction, education and detailed information were included to enable a clear understanding of the broad topic of IT.

Often IT can be misunderstood as the municipality IT resources are not limited to computers, servers and software. IT resources extends beyond into plans, budgets, actions, documents in addition to the physical resources for data storage, protection and much more that aid in operations. IT is an ongoing and constantly evolving facet of municipality operations which should be evaluated at least on an annual basis. IT includes the baseline of an Information Technology Plan (capabilities), Budgeting (planning) and Framework (structure/infrastructure) which is the foundation for fundamentals to function as needed.

A town administrator (TA) or the equivalent role, referred to as TA from here forward typically has the responsibility to oversee and review the Information Technology Plan, Budgeting and Framework for the municipality. This oversight is not limited to the IT infrastructure currently in place but also the future needs of the community. The TA has the responsibility to be the decision maker regarding risk prevention and mitigation, emergency response, and the proactive essentials ensuring that the best interests of the community are addressed. An objective of any Information Technology Plan is having the abilities to identify areas of improvement and do something about it or make a decision of future approach.

The Information Technology (IT) Plan should outline the capabilities required for municipality mission critical services and functions, and Operational requirements. Current and Future State IT infrastructure should be evaluated including but not limited to oversight, procurement, support/maintenance and lifecycle as part of the municipality business continuity plan. Annual evaluation can identify gaps to be addressed and incorporated in to municipality budgeting for initial investments, ongoing support or unforeseen issues. Organizational structure and IT Policies, procedures and processes should be defined so that Roles and Responsibilities may be defined and understood.

Document Description

IT Best Practices for small municipalities is written to be a resource and a reference document to share information with Town Administrators, other decision makers and staff to educate them on many aspects of IT that need to be considered when making decisions for current and future municipality needs. It is a reference guide with checklists, information, reasoning and suggestions to how best implement IT best practices.

The document is segmented into 4 parts as defined below:

Part I:

- Background/Fundamental information
- Checklist(s)

Part II:

- IT Best Practices Guide

Part III**:**

- Appendices

Part IV:

- Glossary

Background/Fundamental information

This section is provided for familiarity to introduce what is IT, what is an IT Plan, procurement insight and using the IT Process Loop to maintain a municipal IT Plan. Small municipalities often struggle with IT resources due to loose management, lack of adequate knowledge and frequent staffing changes. A sampling on a Municipality point of view is included in the Small Municipality, MA sample IT information provided. The Background/Fundamental information attempts to alleviate the struggles by sharing insight to these situations.

- What is IT to a small municipality?
- Common IT resources for small municipalities
- What is an IT Plan?
- Considerations when creating an IT Plan
    - Small Municipality, MA sample IT information provided
- Procurement of IT resources
- IT Process Loop
    - Year 1 IT Plan
    - Using the IT Process Loop to refine the IT Plan
    - Updated Small Municipality, MA sample IT Plan
    - Figure 1: IT Process Loop

Checklist(s)

The checklists serve as evaluation templates to aid in identification of What? Why? How to address? And What is the best practice? They include information to introduce key concepts, considerations and prerequisites to enable the decision-making process while not being an Information Technology specialist. Introduction, education and detailed information were included to enable a clear understanding of the broad topic of IT.

The checklists have statements (fundamentals) or segmented questions (evaluation) for each aspect, a scoring guide (Yes, No and Not Sure – with points as applicable) and detailed links to corresponding sections in the IT Best Practices Guide.

> The Fundamentals of an IT System checklist are the foundation of the municipal business continuity plan, the IT Plan and the Annual IT Assessment.
>
> The Annual IT Evaluation Checklist is a guided inquiry to review the pieces of the current IT systems. The IT systems are enhancements to the Fundamentals and should be evaluated annually.

- Checklist Item
- Example of Checklist Item: Internet Connection
- Internet Connection
- Fundamentals of an IT System Checklist
- Annual IT Evaluation Checklist

IT Best Practices Guide

The guide is not a book to be read and memorized instead it is a resource to support the understanding and interpretation of the checklist and give insight to the questions to enable decisions.

- Assets
- Risk
- Data Protection
- Data Security

Appendices

- Appendix 1: Information Technology Policy
- Appendix 2: Resource Tracking Record
- Appendix 3: White and black lists
- Appendix 4: Inventory data collection tool
- Appendix 5: Access Control Policy
- Appendix 6: Procurement guidelines
- Appendix 7: Town of Conway IT Best Practices Policy Statements

Table of Contents

Part I: Background/Fundamental information

What is IT to a small municipality?

IT is the foundation for many day to day operations in most small municipalities. Often IT can be misunderstood as the municipality IT resources are not limited to computers, servers and software. IT resources extends beyond into plans, budgets, actions, documents in addition to the physical resources for data storage, protection and much more that aid in operations. Plans and budgets must consider the current and future physical resources, the information used, gathered, transmitted and stored, the importance of the varying information, the maintenance and its related costs of the physical and virtual resources.

IT can include Computers, Copiers/Printer, Public Wi-Fi in town buildings, Police/Fire and EMS support services, Phone Systems and more. IT is not only tangible items it is the data, the passwords, the software, the infrastructure that enables the data to be transmitted, collected, stored and recovered when needed. There are common IT resources used in most municipalities to provide fundamentals of an IT system.

Small municipality IT is typically managed by an overarching ongoing IT Plan. This plan is compiled by the town administration who will do their best make the decisions in the best interest of the municipality in the immediate time frame and the future. Although the town administration changes frequently the IT infrastructure must be stable and well thought out. Small municipalities struggle with the necessity of IT infrastructure and the ability to consistently address the concerns of security, data integrity and cost savings. These struggles can be identified, documented and addressed with an ongoing IT Plan. Many small municipalities find themselves at a critical juncture with regard to technology. Variances in equipment, software and age along with substandard infrastructure require significant and meaningful long-term changes to IT systems.

Common IT resources for small municipalities

Although the computer landscape in most small towns is very basic, there are common IT resources, related services and functions that each municipality should have. These fundamentals not only include the computers but the internet connection, passwords, Wi-Fi, anti-virus, email and file backups. The following common resources are identified and common pitfalls often overlooked by municipalities are provided for clarity.

Computers, Internet Connection, Passwords

These important resources including computers vary from age, type, operating systems and more. A network shares an internet connection between resources, be it more than one computer or a printer/copier and are often used in small municipalities. If passwords are in use, they are usually very basic and not changed very often. In most cases the passwords have been in use for years, and are commonly written somewhere close to the computer. Either on a sticky note on the monitor, under the keyboard or on a desk planner. When a computer or account is used by multiple people, the username and password is often shared. This usually prolongs the password from being changed unless the account (website or similar) enforces it. It's not uncommon for the passwords on shared accounts to outlast the employment of the people who use them.

The loose management of these resources affects accountability, accessibility and most importantly susceptibility to negative situations. Unmanaged, uncontrolled and insecure passwords greatly increase the chance for unauthorized access to systems or confidential data. Passwords are commonly reused, so the computer login password, could be the same that is used for email or financial systems. Shared user accounts reduce accountability, and the outdated, unprotected computers increases the risk of hardware failure and susceptibility to viruses and hacking.

Wi-Fi

The loose management is often carried over to the commonly found municipal Wi-Fi network where the default password and management settings have not been changed from the manufacturer. This password is usually commonly known and shared, often posted in public space, however in most cases, the Wi-Fi and local computers all connect to the same network. Anyone on the Wi-Fi, even a "guest" may have access to all the municipal network assets.

> *The State provided computers are the only computers that are separated from the Town's network. They are usually in the clerk's office and have their own internet connection and printer. Getting information off of these computers to share is intentionally difficult. USB drives are blocked and the most common way to get data is to print it, or burn it to a CD/DVD. Police departments typically utilize a separate network, as a requirement to get access to Criminal Justice Information Services (CJIS).

An unencrypted wireless network, without a password, is exposed and all data transmitted can be seen and this would be similar to trying to have a private conversation on a public bus. Anyone within earshot could hear the contents of your conversation. The potential for the web browsing and email content being viewed by others is real.

Unauthorized devices can access the Wi-Fi, and if not managed the internet speed can be compromised, by extra connected devices, additionally there is an increased chance of data theft or virus infections. A computer that is on a network, can potentially gain access to confidential data. It is trivial to run automated attacks to break passwords, install monitoring software or other types of malware.

Anti-virus

In many small towns, the anti-virus is managed on a per computer basis. Most computers are using a free anti-virus software such as Microsoft Security Essentials, AVG or Avast. These packages, while free, are technically not licensed for government or commercial use. There usually isn't any maintenance or review of the software. It is installed and left alone unless a pop-up message occurs.

Using unmanaged anti-virus software creates a false sense of security. Due to its presence, it is assumed that the computer is fully protected. However, without periodic checks, it is unknown if the software is running properly, up to date or if any infections were found. The typical threats like malware often disables or attacks anti-virus software leaving the user unaware of any issues. Without a centralized antivirus, computers that are missing anti-virus software are often missed. Many times, computer users are unaware that there isn't any anti-virus software installed on their machine.

Email

Email platforms in use are usually mixed from within the Town. The Police, Water and Highway departments often have their own domains (townpolice.com, townhighwaydept.com vs town.ma.us or townma.com) and email providers. Other times the company providing the internet is used for the email host, such as Comcast, Verizon or Crocker. It is recommended that municipalities create .gov email addresses for staff (see Data Protection – Email Security)

Email is often a basic service and does not include archiving or email sync capability. New email is downloaded to the computer and is stored locally. In the event of a computer failure, all email is lost. With employee turnover, email from previous employees is often lost or not transitioned very well. Sometimes new employees will use the previous persons email to try to avoid this. In this situation, a user "John" will be signing in and sending mail as the old Town employee "Dave". This adds confusion but is often ignored as it easier then losing mail.

Data backup

Data backup is done either with a cloud service such as Carbonite or Mozy or manually with an external drive or USB flash drive. The data selection of what is backed up is often not really known and was often done or setup by someone else and is just assumed that it is done. In the event of a computer failure, there is not a plan on what to do. Hopefully the person who set the backup would be available to assist.

Manual backups rely on individuals to remember and get in the habit of backing up. It's often something that falls through the cracks as other office duties and life issues distract the person responsible. It is a task that has no reward or direct value on a regular basis. Backup and recovery are only important if a data disaster occurs and until that event takes place, and is often an afterthought.

The likelihood of data loss when a disaster takes place increase when what and how data is backup greatly increases when not routinely checked. Once again users having a false sense of security with the assumption of when the backup was setup, it was configured to protect all important data., by the setup person. Just the presence of having a backup of any kind implies to users that they are protected. Often the initial setup of the backup system is not done by a people who is familiar with all the systems and data the Town needs. They do their best to make a judgement call on what should be backed up and the backup frequency, which may or may not be the correct configuration for the Town.

What is an IT Plan?

An IT plan is a comprehensive snapshot of municipality Information Technology, it can be a very useful document with history and information if maintained correctly. An IT Plan can offer great insight to the current state and future state of municipality Information Technology as well as the history. It can manage and direct resources to support strategy and priority of the municipality. A foundation of any Information Technology Plan is having the abilities to:

- identify areas of improvement
- do something about it or make a decision of approach.

If the municipality does not have the ability (Internal) or resources (External) to support the needs of the community, the plan will be incomplete. If the ability is not possessed, the appropriate organization that does needs to be brought in for guidance.

The IT Plan should outline the capabilities required for municipality mission critical services and functions, and Operational requirements. The Plan should be a living document that guides the municipalities decisions for funding, captures the decisions made, as well as the details of the decision-making process used. This plan can be used for budgeting purposes for the current fiscal year and the future if documented correctly. An IT plan can focus the efforts of the review committee by having complete notes available for review. If the lifecycle of a piece of hardware is sufficiently noted in the IT plan with enough information to clearly understand the lack of necessity to review this piece of hardware the review can be expedited.

> *Example of procurement information that should appear in an IT Plan:*
>
> *The server (X hardware) was replaced in November 2016, the review/replacement can be passed over for 36 months (through November 2019) as the maintenance and monitoring process ensures the functionality and adequacy of the hardware.*

Considerations when creating an IT Plan

An IT Plan should include information regarding the IT infrastructure what is included (ownership, location, accessibility, responsibility), when was it purchased, what is needed to complement and expand the coverage. Has standard hardware and software requirements been identified and captured in the IT plan for future purchase guidance?

An IT Plan should identify the applications suite standard that has been selected (i.e.: MS Office) and standardized. If an email platform has been selected and implemented the requirements and configuration of accounts should be documented in the Plan.

Any information regarding the Internet Connection should be captured and maintained as upgrades occur as the security of the connection must be maintained as it may be used for data transmission and more, including:

- Use of State websites for data entry (Department of Revenue) and information sharing (Mass. Emergency Management Agency's "e-EOC" or electronic Emergency Operations Center)
- Links to external sites (e.g., Cartographic Associates for GIS; the FRCOG's accounting system; the Massachusetts Municipal Association and perhaps other municipal organizations)
- Web browsing
- Management of municipality website

Additional resources are provided by the state for some functions – i.e.: State computers for the Town Clerk and Police. There are some optional IT aspects that may be included in the IT Plan:

- Optional (Town specific): Payroll processing
- Optional: VPN remote access or equivalent accessibility
- Optional: VOIP, voicemail to email capability

If an external resource, i.e.: An Outsourced IT firm has an established relationship with the municipality and has insight into the infrastructure and purchase requirements this should be noted in the IT plan as well. If identification of essential functions and the required IT has been completed, it should be captured in the plan. What are these day to day functions and mission critical services and functions that have been identified, what are the capabilities required to maintain these functions and services.

If critical failure points have been identified, have they been documented, including the possible failure mechanisms, i.e.: without oversight, back up or unidentified ownership? Information Technology projects in work should be documented include the outline of the upgrade plan, where in the allocation cycle the municipality is at, if grant funds are available and in use what are the restrictions and guidelines.

Documentation of procurement decisions should be captured in detail.

> *Example of procurement information that should appear in an IT Plan:*
>
> *A server was purchased in 2016 and will need to be replaced in 5 years (2021), two new PCs are to be purchased for the Parks and Recreation Department and the Public Works department in 2017. One PC will be purchased in 2018 for the administration office. The printers are sufficient*

and have been connected to the network via the server, the lifecycle of the printers is expected to surpass 2021 based on historic performance. There was an amalgam of anti-virus software and with the purchase of the two PCs, two new licenses need to be purchased to integrate them to the server that monitors the anti-virus profile and breaches.
The Police Department was not upgraded in 2016 as participation in the assessment was declined, however needs to be evaluated for needs which may include 4 PCs, 4 anti-virus licenses and a new document center for scan, fax and print resources.

An IT Plan should be reviewed and updated upon completion of an Annual IT assessment, i.e.: Small Municipality Annual IT Evaluation if not more often as it it's the foundation for the Business Continuity Plan. Annual evaluation can identify gaps to be addressed and incorporated in to municipality budgeting for initial investments, ongoing support or unforeseen issues.

Current and Future State IT infrastructure should be evaluated including but not limited to oversight, procurement, support/maintenance and lifecycle as part of the municipality business continuity plan. Organizational structure and IT Policies, procedures and processes should be defined so that Roles and Responsibilities may be defined and understood.

Small Municipality, MA sample IT information provided

Small Municipality, Massachusetts has identified a need to review the town Information Technology current status. After an initial evaluation:

Small Municipality, MA current state of Information Technology

- *No IT plan in place, currently or historically*
- *3 computers, varying ages, operating systems*
- *Wi-Fi password posted in the public area of town hall, all assets exposed*
- *No network, no IT support, no backups, no antivirus protection*
- *Each computer has a local printer available*
- *Free email addresses used (i.e.: @gmail.com), basic POP configuration, no backup*
- *Access to MassBroadband 123 network*
- *Police, Fire and EMS Departments*
- *The Public Library which utilizes the appropriates services provided through CWMARS (?)*

This assessment has been completed as a favor to the Town Administration by an IT enthusiast. No formal external IT support has been used to determine IT decisions to date, Small Municipality has been self-supported to date.

- *Verizon currently provides internet access to the computers via a DSL Modem/Router, Password: SmallMuniPass.*
- *Licensing information is unavailable for any of the software found on the 3 computers.*
- *Note: Employees noted the printer ink frequently dries up before used completely.*
- *No surge protection, uninterruptable power supply or otherwise in use.*
- *No policies exist at this time.*

Procurement of IT resources

In an effort to support the Community Compact Initiative which gives Massachusetts cities and towns the chance to make needed improvements through collaboration with and support from the Commonwealth. The state offers incentives for communities that join the effort, including:

- A grant program for Community Compact
- Extra points on certain grants
- Technical resources from the Commonwealth to help communities achieve their goals

Once a municipality has decided that it wants to implement a Community Compact, local government leaders will need to take the following steps: A municipality may apply to focus area, referred to as "Best Practice area" of Information Technology — Areas include cyber security, citizen engagement, and transparency. The process can be reviewed here:

- https://blog.mass.gov/blog/government/the-massachusetts-community-compact-initiative/
- http://www.mass.gov/governor/administration/groups/communitycompactcabinet/

New technology purchases, enhancements and/or replacements should be incorporated into the town's capital improvement program. Capital appropriation requests for technology should be submitted by the Technology Department or the assigned municipal employee responsible for town-wide IT decisions. IT purchases should be subject to the same capital review process as all other town departments. See Procurement guidelines.

Among factors to consider are the age and remaining capacity of units to be replaced; potential department and town-wide efficiencies; compatibility with existing hardware systems; alternatives; and relative costs. Equally important is how a purchase fits into the Town's long-range plan for technology use and enhancement.

Municipality procurement should follow a process that includes ownership assignment, needs assessment, timeline development, research and review. Before making major hardware or software purchase decisions, the town should plan and follow an internal process similar to the following.

a. Assign responsibility (either internally or externally with an IT consultant) for assessing need and receiving staff input
b. When acquiring new hardware, in bulk or as individual units, the first step involves assessing need and intended use.
c. Develop a timeline by establishing a full installation/fully operational target date and then work backwards. As part of establishing a fully operational target date, decide if old and new systems are to run in parallel for any length of time.
d. Complete initial product research, identify vendors, set up product demonstrations or informational meetings.
e. Receive input from end-users (municipal staff), reviews pros and cons of product options, arrive at a consensus. What is an IT Plan?

IT Process Loop

The IT Plan is part of an ongoing IT process as the plan is a living document. This IT Process can be departmentally owned or collectively owned - no matter the ownership it is suggested that the reasons for decisions are formally captured in the IT Plan to transfer the knowledge forward as the players change. Using the Small Municipality, MA sample IT Plan as a starting point the IT Process Loop will be followed and the Small Municipality, MA IT Plan will be updated. When the IT Process Loop begins basic boundaries of budget, departments, physical location(s) are provided.

Initial Evaluation(s)

It is suggested that to determine the current state the Fundamentals of an IT System Checklist and the Annual IT Evaluation Checklist are completed; then the team can conduct Gap Analysis and identify the next steps.

As noted the boundaries of budget, departments, physical location(s) are provided.

- Budget: Small Municipality, MA applied for a 2018 IT grant of $50,000 for IT Infrastructure
- Departments: All departments including Police, Fire and EMS, Public Library any resources not handled by CWMARS.
- Physical Locations: Town Hall, Public Safety Complex

Gap Analysis

Gap Analysis uses the results of the Checklists to identify areas of improvement and possible solutions to do something about it or identify an approach to address the gaps.

The Gap Analysis results in identification of the following deficiencies:

- IT Details (Network, infrastructure, hardware, software) Current State: see Small Municipality, MA sample IT Plan
    - The IT Infrastructure including data cabling, firewall, network switches were found to be sufficient for the current needs of the municipality, however the capacity is maxed out.
    - A terminal server implementation (with supporting servers) is recommended
- Departmental IT Needs/Information
    - Business class router
    - Secure Internet and Public Wi-Fi
    - A server environment
    - Archived or Sync Based Email systems (for all departments)
    - Networked PCs, printers, anti-virus, back up, licensed supported software
- Policies: None
- Project Plans: None in place at this time
- IT Future State: Connection to MassBroadband 123

Compliance – password policy – non-networked – end user responsibility for ensuring security? Is there budget to address baseline gaps? $50K for IT infrastructure?

Decision-Making Process

With the information provided from the Gap Analysis, a decision-making process is initiated.

Upon completion of the Committee review the following decisions were made for a 3-year IT plan

Year 1: Infrastructure update – increased capability and security

- Firewall/ switches/anti-virus, Wi-Fi – business class
- Printers (Laser Jet from Ink Jet) – Digital copier/Document Center
- Computers – OS, AV, productivity SW

Year 2: Server Implementation – ease of management of IT resources, centralized data location, lower risk of data loss, Increased network security -

- Server
- Defer connection to MassBroadband123 – cost prohibitive ($130/ monthly cost)

Year 3: Maintenance and monitoring plan

- Signed support agreement
- Hire an IT professional

Budgeting Process

Departments should be responsible for overseeing IT hardware/software needs and recommending expenditures through the Operating Budget or Capital Budget.

Year 1: ~$18K budget allocation.

- $1K Firewall/ switches/anti-virus, Wi-Fi – business class
- $15K/ (lease option) Printers (Laser Jet from Ink Jet) – Digital copier/Document Center
- $ 2.4K Computers – OS, AV, productivity SW
    - Archived or Sync Based Email systems

Year 2: $50K for IT infrastructure for 2018

- The IT Infrastructure including data cabling, firewall, network switches have been upgraded in previous year as part of this Plan and were found to be sufficient for needs of the municipality.
- $30K A terminal server environment implementation is recommended
    - Labor to implement server environment
- $ Networked PCs, printers, anti-virus, back up, licensed supported software

Implementation and Installation

After the initial pass through the IT Process Loop the process begins again with the information gained from the first pass.

The documentation created should identify the next steps of the process, compliance, technology solutions, pricing, policies, oversight, etc. The starting point for the next pass through the loop (continuous IT evaluation) is now defined.

Year 1 IT Plan

The Year 1 IT Plan is a compilation of evaluation – including the checklists, gap analysis, decisions, budget considerations to determine a comprehensive snapshot of the structure/infrastructure with consideration of capabilities needed and accessible budget.

The identification of the path forward based on these decisions, budgeting and the implementation and installation should be captured to ensure the Plan is a useful resource currently and in the future and accurately reflects the history. It is beneficial to identify and capture the following in the IT Plan

- What deficiencies were identified and addressed immediately?
- What deficiencies need to be revisited in the future?
- What has been accomplished to date?
- What is planned to be accomplished?
- What is on hold, out of budget, next steps?
- Why were priorities selected?
- When is next evaluation period?

Using the IT Process Loop to refine the IT Plan

Year 1 - Competed X, Y, Z

Year 2 – Annual IT evaluation

Gaps from year 1 gone, except end user security

New Gaps identified – Maintenance and monitor

Updated Small Municipality, MA sample IT Plan

Small Municipality, MA completed its initial evaluation to identify the current state of Information Technology in the community

- *A 3-year IT plan is in place*
- *A terminal server was implemented in 2017 and will need to be replaced in 5 years (2022)*
- *3 computers have been connected to the server with anti-virus, back up, licensed supported software*

- *Secure internet and public Wi-Fi have been established*
- *New network established*
- *IT support contract to monitor backup and anti-virus*
- *Backups and anti-virus protection implemented*
- *Printers have been networked and can be shared, but are still collocated with each computer*
- *A business class email platform with email archiving was implemented for all departments*
- *Access to MassBroadband 123 network is available but not implemented as too expensive to connect at this time.*
- *Police, Fire and EMS Departments (integrated to internet, network, email platform, backup and antivirus)*
- *No interaction with The Public Library which utilizes the appropriates services provided through CWMARS (?)*

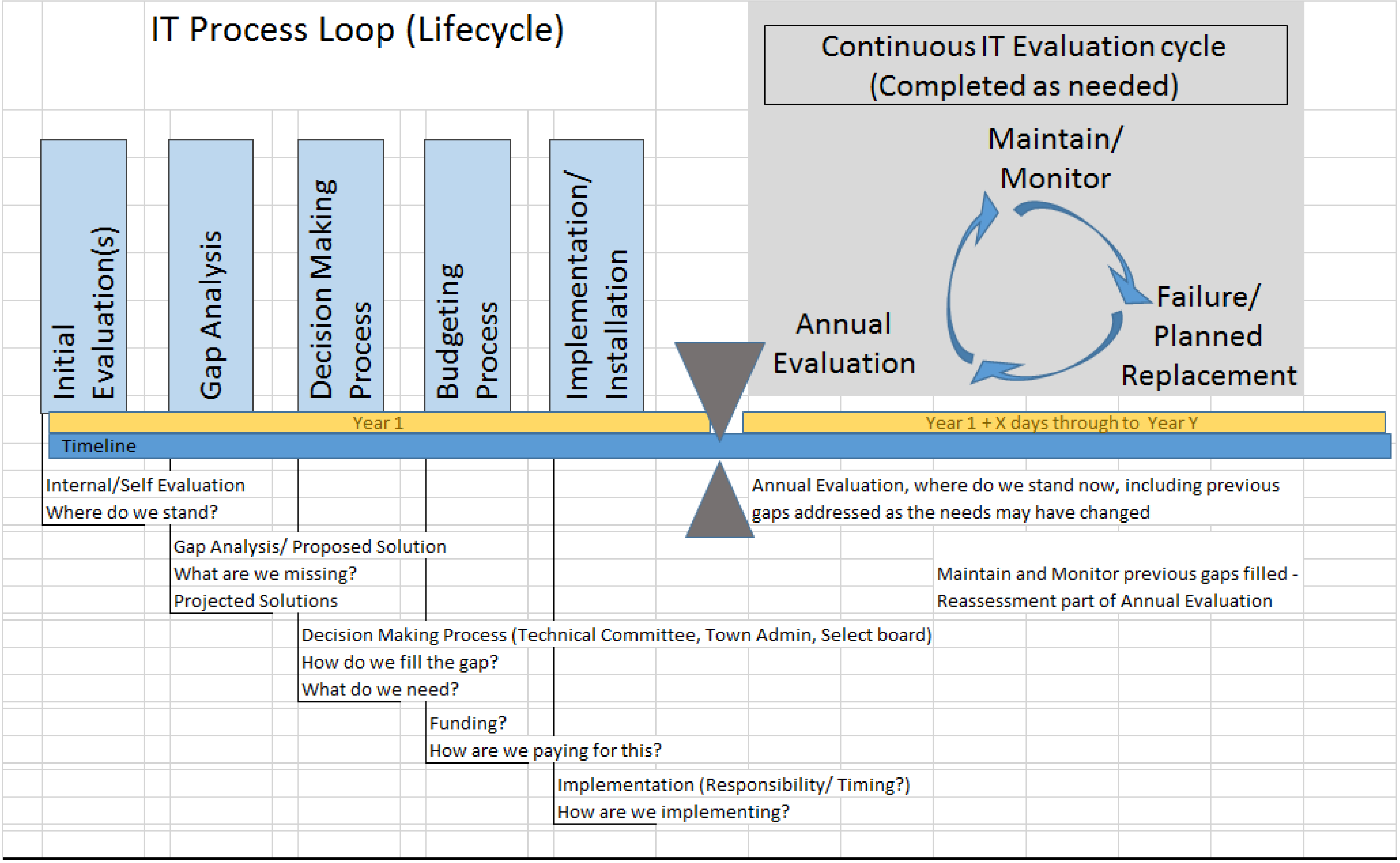
This assessment has been completed by IT4U, a formal external IT support contract to monitor backup and anti-virus has been signed for the next 24 months.

Comcast currently provides internet access to the computers via the firewall, network switches, a Motorola Modem and Linksys Wireless Router

Licensing information is up to date on the 3 computers.

Note: Employees noted the printer ink frequently dries up before used completely.

Surge protection and uninterruptable power supplies were put into use.


IT Process Loop (Lifecycle)
Continuous IT Evaluation cycle (Completed as needed)
Initial Evaluation(s)
Gap Analysis
Decision Making Process
Budgeting Process
Implementation/ Installation
Maintain/ Monitor
Failure/ Planned Replacement
Annual Evaluation
Year 1
Year 1 + X days through to Year Y
Timeline

Internal/Self Evaluation
Where do we stand?

Gap Analysis/ Proposed Solution
What are we missing?
Projected Solutions

Decision Making Process (Technical Committee, Town Admin, Select board)
How do we fill the gap?
What do we need?

Funding?
How are we paying for this?

Implementation (Responsibility/ Timing?)
How are we implementing?

Annual Evaluation, where do we stand now, including previous gaps addressed as the needs may have changed

Maintain and Monitor previous gaps filled - Reassessment part of Annual Evaluation

Figure 1: IT Process Loop

Part I: Checklist(s)

Checklist Info

The Checklists were developed to objectively and critically review the IT a small municipality health.

An IT Plan evolves from fundamentals to elaborately complex IT systems. The Fundamentals of an IT System checklist are the foundation of the municipal business continuity plan, IT Plan and the Annual IT Assessment.

Each item identified in the checklists are covered in detail in the IT Best Practices Guide, which is provided to aid interpretation of the checklist. Each item on the checklist has the following descriptors: Statement, Scoring, Corresponding IT Guide Section for more information listed on the Checklist.

The explanation for each item is consistently formatted:

Checklist Item

What is the Checklist Item and its' application?

Why is it important?

If applicable: Features/Aspects, Details

How to address? What is the best practice?

Recommended paths: Best, Better and Good

If applicable: Level of Tolerance/Risk, Relative Cost/Budget

Example of Checklist Item: Internet Connection

Internet Connection

What is it and its' application?

Internet Connection - This must be a constant high-speed connection that provides access to email, software updates and other critical services. *

> *There can be variability in the requirement if the offices are not all co-located and unable to share a connection and no critical data is stored or contained a lesser connection may be acceptable.

Why is it important?

The internet connection is an important operational requirement as it affects and facilitates many aspects of municipality. It provides access (collection, containment and storage) to information, communication between departments, personnel, external agencies, etc. and much more.

How to address/What is the Best Practice?

A constant high-speed connection can be sourced in multiple ways recommendations are listed below:

Best: Fiber Connection, such as Massachusetts Broadband Institute (MBI) if it is not cost prohibitive for the municipality to own/operate a broadband network.

Better: Cable (shared in the neighborhood) for non-critical data this connection may be acceptable for

Good (Not recommended): DSL (recommended min 1.5MB/s) connection for non-critical data this connection may be acceptable for satellite offices.

> ***Example:*** *The municipality of Rowe was provided with an MBI connections, but continues to use DSL for the conversion to MBI usage infrastructure was cost prohibitive.*

Fundamentals of an IT System Checklist information

The Fundamentals of an IT system checklist was limited to 5 major categorical topics to gauge the infrastructure. An Internet Connection is an Operational Requirement for an IT system however it must meet criteria as defined in the detailed section in the guide. Anti-Virus (Licensed) on all Computers, Computers running up to date (vendor supported) software, File Backup, and Strong passwords are foundational recommendations for data protection. The Data Protection section is extensive and many other aspects of data protection are included however the foundational recommendations of the Fundamentals of an IT system are listed first.

Fundamentals of an IT system (Minimum Operational Standards)						IT Guide Section	Pts
1	**Internet Connection** A constant high-speed connection that provides access to email, software updates and other critical services, such as web-based applications.		□ Yes 10 Pts	□ No	□ Not Sure	Assets – Internet Connection (Page 27)	
2	**File Backup** All critical data are regularly backed up in some fashion.		□ Yes 30 Pts	□ No	□ Not Sure	Data Protection – Backup and Recovery (Page 40)	
3	**Strong Passwords** Passwords are subject to formal rules on format (number of characters, case, numbers and symbols) that apply town-wide and the passwords are changed regularly, non-duplicated, and protected.		□ Yes 25 Pts	□ No	□ Not Sure	Data Security – Access Control (Page 47)	
4	**Anti-Virus (Licensed) on all Computers** Free antivirus (versus paid subscription) options such as AVG or Microsoft Security Essentials not licensed for Commercial or Government use do not meet the requirement of a "Yes" response.		□ Yes 20 Pts	□ No	□ Not Sure	Data Security – Protective Technology (Page 47)	
5	**Computers running up-to-date (vendor supported) software** Regular, proactive downloading and installation of software updates for the current version (not version upgrade) regularly or are automated for each software application (Operating system, browser, third party software, etc.)		□ Yes 15 Pts	□ No	□ Not Sure	Data Security – Maintenance and Monitoring (Page 48)	
						Total Pts	

Annual IT Evaluation Checklist information

Annual IT Evaluation Checklist is a guided inquiry to review the pieces of the current IT systems. The IT systems are enhancements to the Fundamentals and should be evaluated annually.

Assessment of the IT systems ensures the best practices are in place where feasible, identifies gaps in the current IT systems. Identification of immediate needs, missing information, lost resources, etc. Recommendations for purchases and resource can be a result of the assessment as could expansion an existing IT project as it meets a newly identified need

IT Plans evolve from fundamentals to elaborately complex IT systems. The Fundamentals of an IT system checklist are the foundation of an IT Plan and the Annual IT Assessment. The Fundamentals include:

a. Internet Connection
b. File backups
c. Strong Passwords
d. Antivirus
e. Up to date software

The fundamentals support the common IT related services and functions

An Internet Connection is an Operational Requirement for an IT system however it must meet criteria as defined in the detailed section in the guide. Anti-Virus (Licensed) on all Computers, Computers running up to date (vendor supported) software, File Backup, and Strong passwords are foundational recommendations for data protection. The Data Protection section is extensive and many other aspects of data protection are included however the foundational recommendations of the Fundamentals of an IT system are listed first.

Section 1, Annual IT Evaluation Checklist: Asset Management					IT Guide Section	Pts
1.1	Is there an accurate detailed inventory of hardware?	□ Yes 20 Points	□ No	□ Not Sure	Assets – Asset Management – Inventory data collection (Page 34)	
1.2	Is there an accurate detailed inventory of software?	□ Yes 20 Points	□ No	□ Not Sure	Assets – Asset Management – Inventory data collection (Page 34)	
1.3	Is there a scheduled/periodic review of hardware and software to update the inventory?	□ Yes 10 Points	□ No	□ Not Sure	Assets – Asset Management (Page 31)	
1.4	Is there a hardware replacement schedule in place?	□ Yes 15 Points	□ No	□ Not Sure	Assets – Asset Management (Page 31)	
1.5	Is there a software replacement/upgrade schedule in place? (General - MS Office, departmental level (SoftRight, VADAR, Point))	□ Yes 10 Points	□ No	□ Not Sure	Assets – Asset Management (Page 31)	
1.6	Is there central oversight of IT expenditures?	□ Yes 20 Points	□ No	□ Not Sure	Assets – Asset Management (Page 31)	
1.7	Is there an established protocol for annual IT expenditures, whether through the operating budget or capital budget?	□ Yes 15 Points	□ No	□ Not Sure	Assets – Asset Management (Page 31)	
					Section 1 Total Points	

Section 2, Annual IT Evaluation Checklist: Data Security					IT Guide Section	Pts
2.1	Is there confidential information stored on the IT system?	□ Yes 0 Points	□ No 10 Points	□ Not Sure	Data Security – Confidential Information (Page 52)	
2.2	Is town owned Confidential information stored on electronic devices (i.e. laptop, cell phone, tablet, etc.) permitted to be removed from municipality premises? If Yes, describe authorization & control measures on a separate sheet.	□ Yes 0 Points	□ No 10 Points	□ Not Sure	Data Security – Confidential Information (Page 52)	
2.3	Is authorized remote access to the town network and town computers permitted?	□ Yes 0 Points	□ No 10 Points	□ Not Sure	Data Security – Remote Access (Page 51)	
					Section 2 Points Subtotal	

Section 2, Annual IT Evaluation Checklist: Data Security					IT Guide Section	Pts
2.4	Does the town accept credit cards for bill payments? If No, skip to question 2.5	□ Yes 0 Points	□ No 10 Points	□ Not Sure	Data Security – Confidential Information (Page 52)	
2.4.1	If yes (to question 2.4), does the town have data and system protection agreements with any third party that accepts credit card payments on behalf of the town?	□ Yes 10 Points	□ No	□ Not Sure	Risk Assessment – Risk prevention, mitigation and tolerance (Page 36)	
2.5	Does the town assign staff permission levels that allows or restricts access to electronic data?	□ Yes 15 Points	□ No	□ Not Sure	Data Security – Access Control (Page 47)	
2.6	Are there known deficiencies in the security practices of the municipality? If No, skip to question 2.7. If deficiencies are identified, please detail the deficiencies and resolution on a separate sheet	□ Yes 0 Points	□ No 10 Points	□ Not Sure	Data Security (Page 46)	
2.6.1	If there are known deficiencies in the security practices of the municipality are there resolutions identified?	□ Yes 10 Points	□ No	□ Not Sure	Data Security (Page 46)	
2.7	Are all users with access to systems are authenticated by means of unique and individually assigned passwords, physical characteristics or digital ID?	□ Yes 10 Points	□ No	□ Not Sure	Data Security – Access Control (Page 47)	
2.8	Is access to network or data controlled by role-based authentication rather than name based authentication?	□ Yes 5 Points	□ No	□ Not Sure	Data Security – Access Control (Page 47)	
2.9	Does the municipality allows the use of file sharing or Peer-to-Peer networking technology?	□ Yes 0 Points	□ No 10 Points	□ Not Sure	Data Security – Access Control (Page 47)	
2.10	Does the municipality have secure storage areas (i.e. locked rooms, locked file/server cabinets, limited access areas, etc.) for documents containing customer and/or employee personal identification information?	□ Yes 10 Points	□ No	□ Not Sure	Data Security – Physical Security (Page 51)	
2.11	Have you identified a person or party to determine the municipality risk tolerance levels?	□ Yes 10 Points	□ No	□ Not Sure	Risk – Assessment: Risk prevention, mitigation and tolerance (Page 36)	
					Section 2 Total Points	

Section 3, Annual IT Evaluation Checklist: Monitoring and Maintenance						IT Guide Section	Pts
3.1	Is there an established relationship with an external IT professional or IT firm to provide ongoing and emergency technical support?		□ Yes 15 Points	□ No	□ Not Sure	Data Protection – Backup and Recovery (Page 40)	
3.2	Are there protocols or steps the staff are directed to take, in the event of a data breach?		□ Yes 5 Points	□ No	□ Not Sure	Risk Assessment – Risk prevention, mitigation and tolerance (Page 36)	
3.3	Is an audit trail that documents user activity (passwords and permissions) maintained?		□ Yes 10 Points	□ No	□ Not Sure	Data Security – Maintenance and Monitoring (Page 48)	
3.4	Are Firewalls, Spam Filters, Virus Protection etc. in use and updated automatically or at least quarterly?		□ Yes 15 Points	□ No	□ Not Sure	Data Security – Maintenance and Monitoring (Page 48)	
3.5	Is there a scheduled/periodic review of software updates and patches?		□ Yes 15 Points	□ No	□ Not Sure	Data Security – Maintenance and Monitoring (Page 48)	
3.6	Does the municipality have secure email practices (i.e., automatically scans and filters emails)?		□ Yes 10 Points	□ No	□ Not Sure	Data Protection – Email Security (Page 44)	
3.7	Is there a Network intrusion detection moitor? If No, skip to question 3.8.		□ Yes 5 Points	□ No	□ Not Sure	Data Security – Protective Technology (Page 47)	
3.7.1	Is there a protocol for responding to a Network intrusion detection alert?		□ Yes 5 Points	□ No	□ Not Sure	Data Security – Protective Technology (Page 47)	
3.8	Is there an Antivirus software virus detection monitor? If No, skip to question 3.9.		□ Yes 5 Points	□ No	□ Not Sure	Data Security – Data Compromise/Loss (Page 51)	
3.8.1	Is there a protocol for responding to an Antivirus virus alert?		□ Yes 5 Points	□ No	□ Not Sure	Data Security – Data Compromise/Loss (Page 51)	
3.9	Is there monitor for multiple failed login attempts? If No, skip to question 4.1.		□ Yes 10 Points	□ No	□ Not Sure	Data Security – Maintenance and Monitoring (Page 48)	
3.9.1	Is there a protocol for responding to a multiple failed login atempt alert?		□ Yes 5 Points	□ No	□ Not Sure	Data Security – Maintenance and Monitoring (Page 48)	
						Section 3 Total Points	

Section 4, Annual IT Evaluation Checklist: Data Backup					IT Guide Section	Pts
4.1	Is a written data back-up plan created and adhered to?	□ Yes 50 Points	□ No	□ Not Sure	Data Protection – Backup and Recovery (Page 40)	
4.2	Is a written data disaster recovery plan created? If No, skip to question 4.3.	□ Yes 25 Points	□ No	□ Not Sure	Data Protection – Disaster Recovery (Page 42)	
4.2.1	Is a written data disaster recovery plan tested through a simulation or exercise?	□ Yes 10 Points	□ No	□ Not Sure	Data Protection – Disaster Recovery (Page 42)	
4.3	Does the municipality back-up network data and configuration of files daily?	□ Yes 15 Points	□ No	□ Not Sure	Data Protection – Backup and Recovery (Page 40)	
					Section 4 Total Points	
Section 5, Annual IT Evaluation Checklist: Regulatory Responsibilities					**IT Guide Section**	**Pts**
5.1	Is a specific data retention/destruction schedule in compliance with MA Public Records law adhered to?	□ Yes 25 Points	□ No	□ Not Sure	Assets – Mission Critical and Emergency Response (Page 28)	
5.2	Does the municipality requires its service providers to maintain at least the same level of data security regimen that it maintains?	□ Yes 25 Points	□ No	□ Not Sure	Data Security (Page 46)	
5.3	Are the Treasurer, TA, and other responsible parties aware of their regulatory responsibilities? For example Ambulance, Fire, etc.	□ Yes 50 Points	□ No	□ Not Sure	Risk – Legal/Regulatory Responsibility (Page 37)	
					Section 5 Total Points	

Part II: IT Best Practices Guide

This guide is not a book to be read and memorized instead it is a resource to support the understanding of the checklist and give insight to the questions to enable decisions.

IT in a small municipality is an ongoing and constantly evolving facet of municipality operations. IT systems have multiple roles in that they can be data repositories, reference tools, brains and more. When managing these systems much care and caution should be used to ensure that the inventory and needs, or the Assets, the exposure to danger, or Risk, and the data protection is done in a way that is sustainable and responsive to the evolutionary cycle of the community or the IT Process Loop

Annual assessment of IT systems should be completed to ensure the needs of the community are being met and the technology is in place to minimize the risk and that the data is protected and secure.

Assets

What do you have? What do you need?

Operational requirements are defined as what the municipality at a minimum must have in place to accomplish daily tasks:

- Internet Connection
- Mission Critical and Emergency Response
    - Critical systems
    - Response planning – timely response to cybersecurity event
    - Incident response and management – discovery/detection, containment, eradicate and recover

Assets – Internet Connection

What is it and its' application?

Internet Connection - This must be a constant high-speed connection that provides access to email, software updates and other critical services. *

> *There can be variability in the requirement if the offices are not all co-located and unable to share a connection and no critical data is stored or contained a lesser connection may be acceptable.

Why is it important?

The internet connection is an important operational requirement as it affects and facilitates many aspects of municipality. It provides access (collection, containment and storage) to information, communication between departments, personnel, external agencies, etc. and much more.

The Internet connection is potentially the Communication link for

- Voice over Internet Protocol (VOIP) – Internet connection and web applications
- Public Safety
- Emergency Services 911

It provides access (collection, containment and storage) to information, communication between departments, personnel, external agencies, etc. and much more.

How to address/What is the Best Practice?

A constant high-speed connection can be sourced in multiple ways recommendations are listed below:

Best: Fiber Connection, such as Massachusetts Broadband Institute (MBI) if it is not cost prohibitive for the municipality to own/operate a broadband network.

Better: Cable (shared in the neighborhood) for non-critical data this connection may be acceptable for

Good (Not recommended): DSL (recommended min 1.5MB/s) connection for non-critical data this connection may be acceptable for satellite offices.

> ***Example:*** *The municipality of Rowe was provided with an MBI connections, but continues to use DSL for the conversion to MBI usage infrastructure was cost prohibitive.*

Assets – Mission Critical and Emergency Response

What is it and its' application?

The IT systems and programs that support critical life and death support systems – i.e.: Public Safety/Health, Communications are considered to be Mission Critical.

Emergency response to a natural disaster or a cyber security event include the plans and actions necessary for timely recovery.

Incident response and management – discovery/detection, containment, eradicate and recover

Critical to town functions are part of the business continuity plan, i.e.: Financial records and Document Management.

This can be the:

- Internet Connection
- Data Storage

Why is it important?

Critical Systems are important as they support Law Enforcement, Fire, EMS, Communications and much more.

Response planning is now just part of our way of life, with ever increasing complexity of cyber-attacks.

Incident response plans needs to be developed in advance of an incident so an organization can discover/detect, contain, eradicate and recover from a cybersecurity event without causing more damage.

The town business continuity plan includes records of town functions – i.e.: Tax Info, Engineering, Vital records, and Payment information. The Data Storage is important as irreplaceable records and permits could be lost.

How to address/What is the Best Practice?

Best:

Identify critical systems ensure proper back up and protective technology is in place to enable timely recovery.

What is the data, where does it reside, is the data backed up?

Document response plans, procedure and process for natural disasters as well as cyber security events. Action plans should be drafted for emergency situations; including but not limited to:

- the loss of the internet resource
- the loss of physical access to a location
- the loss of equipment
- the loss or compromise of data
- the loss or compromise public records (see http://www.sec.state.ma.us/pre/preidx.htm)

The town business continuity plan should be evaluated to ensure proper back up is in place to enable timely recovery

Better:

Identify critical systems understand the recovery process and outline the efforts that it will involve and document the information that may be lost as a result, put in place protective technology.

Discuss and outline the response plan procedure and process for natural disasters as well as cyber security events. Action plans should be discussed for emergency situations; including but not limited to:

- the loss of the internet resource
- the loss of physical access to a location
- the loss of equipment
- the loss or compromise of data
- the loss or compromise public records

The town business continuity plan should be reviewed to understand the recovery process and outline the efforts that it will involve and document the information that may be lost as a result. If backed up on a cycle, ensure that the on-hand records are maintained until the next back up cycle.

Good:

Identify critical systems discuss the recovery process and discuss the efforts that it will involve and the information that may be lost as a result, discuss protective technology.

Discuss the response plan procedure and process for natural disasters as well as cyber security events, as suggested in Better and Best.

The town business continuity plan should be reviewed to ensure that the on-hand records are maintained until necessary.

Assets – IT Policies, Procedures and Processes

What is it and its' application?

IT Policies, Procedures and Processes is the Structure of the Protection Framework.

- Policies are the protocol or guidelines adopted by the municipality in regards to an aspect of IT.
  - Policies are designed to influence and determine all major decisions and actions.
  - All Procedures and processes occur within the boundaries identified in Policy.
- Procedures are the specific methods or official way to express policies in action in day to day operations.
- Processes are the series of actions or steps for the procedures.

Why is it important?

The protection framework clearly defines the structure for Information Technology to assist non-IT professionals in day to day tasks. The documentation ensures continuity in the application of theory upon installation.

How to address/What is the Best Practice?

The Information Technology Policy is the governing document, including the definition of hierarchy of documents and document definitions.

See Information Technology Policy for more information

Best:

All Policies, Procedures and Processes documented

Better:

Some Policies, Procedures and Processes documented beyond those recommended as Good

Good:

At a minimum, the following Policies, Procedures and Processes are documented

- Information Technology
  - IT Policies, Procedures and Processes
- Assets/Asset Management

Assets – Asset Management

What is it and its' application?

Asset Management is the inventory and needs (acquisition, maintenance, lifecycle, etc.) gauge and broken down into three main categories, Hardware, Software, and Inventory data collection.

See specific Asset Management subsections for more detailed information

Expenditures/Budgets

Why is it important?

Asset Management is important because without it there is potential for:

- Acquisition of unnecessary resources
- Improper maintenance and monitoring
- Unknown Loss or Theft
- System and security failures (due to end of life, etc.)
- Licensing fines
- Infection from a known bad software

Standardization, tracking and usage agreement(s) of the Hardware and Software assets is helpful for Asset Management.

See specific Asset Management subsections for more detailed information

How to address/What is the Best Practice?

Maintenance and monitoring is recommended for all hardware and software.

Purchases should be reviewed by a knowledgeable resource to ensure compatibility with the overall network, software programs, etc.

Good (minimum requirement)**:**

Policies, procedures and processes should be defined regarding the usage of Hardware or Software, such as:

- Hardware or Software assignment information (Resource Tracking Record)
- Agreement of Understanding – Signed and Filed

This information should be maintained by one person and/or department.

Assets – Asset Management – Hardware

What is it and its' application?

Hardware is the physical equipment of the IT infrastructure. This is laptops, tablets, phones, desktop, switches or firewalls.

Why is it important?

Hardware standardization in make/models of laptops/workstation and configurations have benefits including support, solutions, response flexibility:

- One vendor to call for support
- Issues/solutions can be applied to all systems
- Ease of required maintenance
- Relocation of asset with similar configuration when critical systems compromised, until resolution

All hardware usage should be tracked, and an agreement of understanding should be signed and filed.

How to address/What is the Best Practice?

Best:

New hardware purchases should be overseen by one person and/or department to ensure compatibility with the overall network, software programs, etc.

CASE STUDY:

The Franklin Regional Council of Government's IT network shares a single operating system and many software licenses. When a new grant was secured that required the purchase of a laptop, the grant administrator ordered the least expensive laptop available. Unfortunately, the laptop's operating system was incompatible with the rest of the FRCOG network. The cost of IT technical support to configure the laptop to be compatible with the rest of the FRCOG network exceeded the cost of the laptop and eliminated all cost savings.

Assets – Asset Management – Software

What is it and its' application?

Software is the programs, applications or "Apps" that are used on the hardware. This can include applications that are available from a CD, downloadable or hosted on the internet.

Proactive downloading and installation of software updates for the current version (not version upgrade) regularly or are automated for each software application (Operating system, browser, third party software, etc.)

Why is it important?

Software standardization (i.e.: uniformity) is important to help reduce support needs and common environment between staff. Benefits include:

- One vendor to call for support
- Issues/solutions can be applied to all systems
- Ease of required maintenance
- Relocation of asset with similar configuration when critical systems compromised, until resolution
- Security

All software usage should be tracked, and an agreement of understanding should be signed and filed. Software requires maintenance for security and relevance.

Software should be purchased:

- In bulk for cost savings and standardized version control of Town-wide software.
- Via volume licenses
- Via subscription model

Volume Licenses:

The single purchase of a software application that can be used by multiple (concurrent) users.

- Expected number of users
- Application specific (routinely or occasionally used)
  - I.e.: Microsoft Office vs. Adobe Acrobat
- Software access via license
  - Many software licenses use the honor system to control the number of concurrent users – the license "key" has no way to lock out users when the maximum number of users are already using the software.
  - Some software volume licenses do prevent users from accessing the software when the maximum number of licenses are in concurrent use. This is typical with specialized and expensive software like ESRI GIS software or some municipal accounting applications.

Subscription Model:

A subscription price is paid for periodic use or access to the software, instead of purchasing the software and reducing the initial upfront cost. Subscription pricing can make it easier to pay for expensive items, since it can often be paid for over a period of time and thus can make the product seem more affordable.

How to address/What is the Best Practice?

Best:

Operating systems (Windows, Mac OS, etc.), productivity software, web browsers all need regular patching and updating to fix vulnerabilities that have been reported (i.e.: Virus protection).

With the implementation of the Better and Good recommendations as well.

Better:

If IT support is to be handled internally, deployment of a network security management tool on internal equipment. This tool will allow the use of (software) application white and black lists.

Good:

Installed programs on municipal resources

- Should be kept to a minimum
- May increase risk exposure due to security flaws
- With an increase of installed programs, feasibility to maintain (patch/update) all is compromised
- Should be documented and recorded
- And activation should align with key/license agreements (quantity)
- Should be monitored for usage/purchase alignment (correct amount/$)
- Should undergo annual audit for license compliance
- Should be reviewed to determine transferability when computers are repurposed to move license to where it will be utilized.

Assets – Asset Management – Inventory data collection

What is it and its' application?

Inventory data collection is the key to proper asset management; it is the identifying information for both Hardware and Software assets.

If a valuation needed to be completed this information would be a foundational piece, as it would provide all the relevant inventory information at a glance.

Why is it important?

Inventory data collection is the key to proper asset management; it is the identifying information for both Hardware and Software assets. Without having the data on the inventory, it is impossible to manage the assets properly.

How to address/What is the Best Practice?

Inventory data collection including all identifying information, assignment information and usage agreements is the key to proper asset management.

Data Collection methods will vary dependent upon the size of your network and can be done:

Best:

Automatic data collections

- Networks greater than 10 computers
- Automated Tool increases efficiency and accuracy of information

A combination of both Automatic and Manual – if some computers out of a large network are standalone, isolated or otherwise manual data collection makes sense for that subset of computers

Better:

Manual data collection

- Networks under 10 computers
- Spreadsheet to document important information, prone to data entry issues
- Must be assigned to a specific person or department and update procedures must be in place and practiced

Good:

Without having the data on inventory, it is impossible to properly manage Hardware and Software assets.

At a minimum, the information identified in the Inventory data collection tool should be captured on a table or spreadsheet.

Risk

What is the exposure to danger of the municipality to cybersecurity risk?

Risk is the exposure to negative circumstances, and due diligence in IT infrastructure and IT plan address both prevention, through avoidance or stopping when detected, and mitigation, the damage control after the exposure.

The Risk Management Strategy should be reviewed annually as part of the Business Continuity Plan.

Risk – Assessment: Risk prevention, mitigation and tolerance

What is it and its' application?

Risk assessment is the understanding of the cybersecurity risk to organizational operations (including functions, image or reputation), organizational assets and individuals.

A municipality can have risk exposure in many ways through its IT infrastructure.

- Data Loss
- Intrusion
- Malicious attacks
- Impacts
- Process identification

Risk Assessment identifies opportunity for exposure prevention, mitigation and tolerance and can be proactive and reactive as necessary.

Risk prevention, tries to stop/avoid the risk before it occurs, and is handled through Data Protection, Backup and Recovery and Data Security. Risk mitigation tries to limit the damage after the risk occurs. Risk tolerance is the willingness to avoid (prevention) or to accept (mitigate) risk. Both prevention and mitigation are essential for demonstrating due diligence in IT Infrastructure and an IT Plan.

A municipality must define and determine its level of risk tolerance, which is usually closely associated with the budget assigned and available. Risk tolerance is a combination of relative importance of data in the infrastructure and ability to recover in a reasonable timeframe with the processes in place.

The following questions will serve as a guide for the definition of a risk management strategy and selection of best practices.

- Importance and Criticality of the data? What is acceptable data loss tolerance?
- Impact of a data breach/leak?
  - Compromised Credit Card information for payments collected
  - Public Records information is public information, not a leak.
- Access to data? Necessity for immediate, how long without access is acceptable?
- What is impact of lost data? Does the process prevent a gap in information?

Why is it important?

Risk assessment is important to ensure the organization understands the cybersecurity risk to organizational operations (including functions, image or reputation), organizational assets and individuals.

A risk management strategy provides a structured and coherent approach to identifying, assessing and managing risk. It builds in a process for regularly updating and reviewing the assessment based on new developments or actions taken. The risk management strategy should identify:

- the "important" data that requires backup systems and corresponding recovery information.
- any redundancies needed.

How to address/What is the Best Practice?

Best practice for risk assessment include adequate preparation, NIST recommended guidelines are:

- Identify and Document Asset Vulnerabilities
- Identify and Document Internal and External Threats
- Acquire Threat and Vulnerability Information from External Sources
- Identify Potential Business Impacts and Likelihoods
- Determine Enterprise Risk by Reviewing Threats, Vulnerabilities, Likelihoods and Impacts
- Identify and Prioritize Risk Responses

This information should be rolled into the risk management strategy, and the procedures and processes should be documented to enable annual review.

Risk – Legal/Regulatory Responsibility

What is it and its' application?

Legal/regulatory responsibilities include if a National Security threat is identified there is a legal requirement to report the information.

HIPPA and Personally identifiable information (PII), any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII and is regulated.

Why is it important?

Threats on National Security are not to be taken lightly

HIPPA and PII regulations require identification and secure handling

How to address/What is the Best Practice?

Best practice for legal/regulatory responsibility include adequate preparation and due diligence

- Identify the responsibilities that are needed to reference the applicable standard(s), common may not apply to all municipalities
    - E.g.: Ambulance – HIPPA
    - Electronic payments (Credit, Debit, etc.) – PCI- DSS

Risk – Device usage/restrictions (see BYOD)

What is it and its' application?

Device usage/restrictions are the guidelines for usage in the workplace and offsite including by not limited to:

- Municipality resources
    - Computer, Laptop, Mobile Devices
    - Printers
    - Internet, email and social media uses
- Personal Resources (BYOD)
    - Computer, Laptop, Tablet
    - Smart phone/Cell Phone

Why is it important?

Without restrictions on resource usage, date could be compromised, computers could be infected or more.

How to address/What is the Best Practice?

Make policy guidelines clear and compliance mandatory.

Policy guidelines should cover the use of features as they relate to work and data.

Risk – Employee Training

What is it and its' application?

Employee training is preparation for performing a job or tasks using the hardware, software and other resources within the guidelines found in the IT Policies, Procedures and Processes.

Why is it important?

Without employee training, there would be not structure to usage of municipality resources.

How to address/What is the Best Practice?

Employee training should be defined for:

- Operational Requirements

  - Employee Onboarding
  - Employee offboarding
- IT policies
  - Access Control
  - Device Usage
  - Remote Access
  - BYOD
  - Data Storage plans

Risk – Bring Your Own Device (BYOD)

What is it and its' application?

Bring Your Own Device (BYOD) is personal equipment that is used for the benefit of another organization, e.g.: smartphone, tablets, laptop and Personal Computers. These are not managed assets.

As consumer products improve, there is an increasing desire for staff members to use their own personal devices for work. This is called BYOD (Bring your own device). While this was most common for smart phone, it has grown to other devices such as tablets and laptops and home PCs.

Why is it important?

Allowing staff members to use their own devices does increase productivity as they are more familiar with these devices. It can also reduce wear and tear on municipality purchased equipment, which can help extend the life and/or reduce maintenance of municipal resources.

Care should be taken when developing a policy for these devices. The Town will not have direct control of the devices, access to sensitive data should be restricted and (on boarding and off boarding) procedures should also be in place to ensure data does not remain on unauthorized devices.

How to address/What is the Best Practice?

Make policy guidelines clear and compliance mandatory.

Policy guidelines should cover the use of features as they relate to work and data.

Data Protection

Data Protection is protection of the data from a logical or physical standpoint is the data backed up, replicated for business continuity and disaster recovery?

Data Protection is defined in the following subsections

- Backup and Recovery
- Disaster Recovery
- Data Storage
- Redundancies

Data Protection – Backup and Recovery

What is it and its' application?

Backup refers to the copying of files/databases to a secondary location for preservation, this enables recovery or the restoration of systems or assets affected by cybersecurity events.

Why is it important?

Data backup is a safeguard against data loss as acceptable data loss tolerance varies with data. i.e.: critical data that is irreplaceable by other means and must be addressed.

Recovery is not only limited to data, but also configurations, software, etc. which can be compromised in a cybersecurity breach. Recovery from a Data Compromise/Loss as a result of an attack, is challenging without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

How to address/What is the Best Practice?

The best practice for backup and recovery of data varies based on the importance of the data. The risk management strategy should identify the "important" data that requires backup systems and corresponding recovery information.

Data identified as Mission critical and for business continuity should be centrally stored and backed up. The most common practice is to store this data on a server and backup that server locally and off site, or as cloud based storage. (However, often times a web based solution is used, which places the backup and maintenance burden on the provider.)

Hard copies of all historical and important data are always recommended where applicable.

The backup plan includes periodic testing of the backup

Best:

Acceptable data loss tolerance and budget will drive the selection of backup systems needed:

- Daily image based Encrypted data backed up on a removable drive, should be stored off site at another Town location.

  IE: Town Hall data drives stored at the Public Safety complex and vice versa.

  Daily capture and weekly rotation of the drive(s), the minimum recommended backup rotation, reduces the hassles. Acceptable data loss tolerance allows for a full week loss of data using this backup system

- Automated offsite file level backup of critical files and database*

  Managed by an IT Firm, with almost full recovery, and provides ongoing and emergency technical support

  **Usually limited to absolutely critical data that is irreplaceable by other means in the event of a local disaster, due to cost.*

Better/Good:

Acceptable data loss tolerance and budget will drive the selection of backup systems needed:

- Daily image based Encrypted data backed up on a removable drive, should be stored off site at another Town location.

  IE: Town Hall data drives stored at the Public Safety complex and vice versa.

  Daily capture and weekly rotation of the drive(s), the minimum recommended backup rotation, reduces the hassles. Acceptable data loss tolerance allows for a full week loss of data using this backup system

- Quarterly archive (provides a snapshot that may be needed in some instances, further back than backup files on hand)

  Implemented using existing backup software, additional expense of additional external hard drives

Data Protection – Disaster Recovery

What is it and its' application?

Disaster recovery (DR) planning is a process that helps organizations prepare for disruptive events — whether those events might include a hurricane or simply a power outage caused by a backhoe in the parking lot.

Why is it important?

A well thought out and designed plan helps to keep important data safe and keep critical services online. This goes beyond data backup, although a good backup plan is part of a DR plan, it extends to include other larger needs.

The main goals of a DR plan are:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

How to address/What is the Best Practice?

The best practice is to identify core/critical data and services such as telephony, internet, tax records etc. that need protection during a disaster and to document that information for reference. A complete plan would include additional locations that can be used as an Emergency Operations or failover. There should be a written plan the describes in detail the equipment needed, responsibilities of staff, and the procedures that should be taken to bring critical services back to operational status.

Best:

A formal written plan is developed

- Risk analysis is performed and critical services and data is identified.
- A second location is selected and prepared for use in case of disaster. This would include preparations for phone and internet capabilities as well as any other infrastructure needs.
- Important data is backup and stored in a safe, dry, secure location
- Staff is trained and an emergency drill is preformed bi-yearly
- DR plan is reviewed annually and updated as needed

  DR Plans are managed by an IT Firm, with almost full recovery

Better:

A formal written plan is developed

- Risk analysis is performed and critical services and data is identified.
- Backups are tested on at least a quarterly basis.
- Staff has reviewed and understands the DR plan
- DR plan is reviewed annually and updated as needed

Good:

A plan is discussed and information is gathered by a point of contact and accessible by others.

- Risk analysis is in work to identify critical services and data.

Data Protection – Data Storage

What is it and its' application?

Data Storage precautionary measures can minimize non-recoverable data loss caused by a virus or hard drive failure when implemented properly.

Why is it important?

Locally stored data on a desktop/laptop computer is not protected from a virus or hard drive failure, and data recovery may not be possible.

Data compromise or loss of irreplaceable records can be devastating for municipalities. Data storage can minimize the impact of compromise or loss.

How to address/What is the Best Practice?

Best:

A Data Storage Plan is defined, implemented and maintained as well as the Better recommendation

Live data storage to a Network Storage System or server is part of a Data Storage Plan.

Better:

For prevention of a non-recoverable data loss, data should be stored on redundant disk arrays such as a NAS (Network Storage System) or a server, if available. This system of multiple hard drives can avoid data loss or corruption in the case of a hard drive failure when configured correctly.

Good:

Critical data is not stored locally only, precautions to replicate the data are taken.

Data Protection – Email Security

What is it and its' application?

Email is information stored on a computer that is exchanged between two users over telecommunications. More plainly, e-mail is a message that may contain text, files, images, or other attachments sent through a network to a specified individual or group of individuals.

Email platforms are tools that support the usage of email by connections provided by email provider, i.e.: the company providing the internet is used for the email host, such as Comcast, Verizon or Crocker. Email is prone to the spread of malware, spam, and phishing attacks, using deceptive messages to entice recipients to divulge sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. Email is also a common entry vector for attackers looking to gain a foothold in an enterprise network and breach valuable company data.

Email security describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise.

Why is it important?

It is the main communication tool for municipality information. It is needed to accomplish most functions.

How to address/What is the Best Practice?

An archived or a sync based system – locally stored and backed up email, to prevent data loss

Secure email practices:

Email security is necessary, and there are multiple measures organizations should take to enhance email security.

- Engage employees in ongoing security education around email security risks and how to avoid falling victim to phishing attacks over email.
- **User accounts**: By functional role versus named users
- **Passwords**: Require employees to use strong passwords and mandate password changes periodically.
- **Encryption**: Utilize email encryption to protect both email content and attachments.
- **BYOD**: Implement security best practices for BYOD if your company allows employees to access corporate email on personal devices.
- **Logins**: Ensure that **webmail applications are able to secure logins** and use encryption.
- **Malware**: Implement scanners and other tools to scan messages and block emails containing malware or other malicious files before they reach your end users.
- Implement a data protection solution to identify sensitive data and prevent it from being lost via email.

Data Protection – Redundancies

What is it and its' application?

Redundancies are a systematic design in which a component is duplicated so if it fails there will be a backup.

Why is it important?

Redundancies are important if an IT component fails.

How to address/What is the Best Practice?

The risk management strategy should address the need for any redundancies identified.

Data Security

Data Security has many facets including the protection framework, policies, procedures, additionally the physical preventative protection measures, i.e.: access control/permission, encryption, passwords, audit logs, etc.

Data Security is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

An example of known deficiency in security practice:

Shared passwords can be a known deficiency - this can be resolved with education and permissions

Data Security is a broad concept that blankets many different ideas and principles including

- Access Control
- Protective Technology
- Maintenance and Monitoring
- Encryption
- Physical Security
- Remote Access
- Data Compromise/Loss
- Legal/Regulatory Responsibility
- Device usage/restrictions (see BYOD)
- Employee Training
- Bring Your Own Device (BYOD)
- Data Storage Plan

Data Security of service providers should be reviewed in cases where information is shared, i.e.: ISP, telecom, banking.

Why is it important?

Data Security is important because without it a municipality may:

- Allow access and modification to important records
- Lose information
- Experience malicious behavior, i.e.: virus, hack, etc.
- Compromise confidential information
- Experience the loss or destruction of equipment
- Expose the entire network to unauthorized access

How to address/What is the Best Practice?

Data security is best achieved through the application of a combination of many principles including:

- Best: Access Control
- Best: Protective Technology – Antivirus product
- Best: Maintenance and Monitoring
- Best: Encryption
- Best: Physical Security

- Remote Access
- Data Compromise/Loss

Data Security – Access Control

What is it and its' application?

Access control is selective restriction of access to network resources, computers, information or files through login credentials or other means of authentication and is the first layer of defense

Permission is granted through User Logins, Accounts and Passwords

Why is it important?

Access control systems perform authorization identification, access approval, and accountability through automated means and permits or restricts access to resources on the internal network.

I.e.: The Town Clerk should not have login abilities to the Treasurer computers' or access to the Treasury files.

How to address/What is the Best Practice?

The consistent implementation of Access Control per Access Control Policy ensures that the network resources, computers or files are secured as it prevents unauthorized access.

The Access Control Policy should include language for:

- User Logins
  - Types
  - Permissions/Security settings
  - Network/Data Access
- User Accounts – Role based accounts
- Passwords
  - Password based access
  - Password requirements
- File sharing or Peer-to-Peer networking, if applicable

Data Security – Protective Technology

What is it and its' application?

IT systems are always at risk and in need of IT support, this can be reduced if protective technologies are installed:

- A maintained Antivirus/Antimalware product can prevent virus and malware attacks.

- An Intrusion prevention system (IPS), a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits, most commonly a firewall is used to automate network security.

Why is it important?

Viruses and malware can infect a resource, or network and cause data loss or more, an Antivirus/Antimalware product can prevent the infection.

An IPS monitors incoming and outgoing traffic and blocks or reports any suspicious activity to ensure network security and prevent threats. They can also filter out some viruses and block known websites that have been detected as malicious. Additional features include content filtering so specific websites or website categories can be blocked.

How to address/What is the Best Practice?

Best:

Good: Firewall, Better: Services/Filtration on Firewall, Best: UTM (Unified Threat Management), Network intrusion - subscription alert (active monitoring)

Installation of protective technologies can reduce required IT support.

- Installation of the Antivirus/Antimalware product noted in Better
- An IPS monitors network security activity
  - Can be automated
  - Filter viruses, and content to block malicious or inappropriate websites

Better/Good:

Installation of an Antivirus/Antimalware protective technology can reduce required IT support.

- A commercially licensed and supported Antivirus/Antimalware product should be installed, Recommended: Sophos or McAfee
  - Networks >5 computers
    - A centrally managed solution should be used
    - Locally installed or cloud based
    - Console for checkup, management, security and settings
  - Networks <5 computers
    - Manual review for checkup, management, security and settings

  Routinely checked to ensure definitions, programs, and user and license agreements are up to date, as well as review logs to look for infections or suspicious programs

Data Security – Maintenance and Monitoring

What is it and its’ application?

Maintenance and monitoring includes review of Asset Inventory (Hardware and Software), Backup/Audit Logs, and Network Configurations. The following pieces of the IT infrastructure require a form of maintenance and monitoring:

- Hardware and Software
  - Backup systems
  - Antivirus/Antimalware products
  - IPS
  - Firewalls
  - Spam Filters

Why is it important?

If any part of the IT infrastructure is not maintained it can destroy the integrity of the entire IT infrastructure by risk exposure.

Maintenance of Hardware/software is required to keep both secure and up to date. Maintenance of hardware can be physical, such as dusting to prevent overheating as well as software updates.

Software requires patches or security updates from the vendor (Supplier - Software Company). Some updates are automated, however not all are.

- Maintained manually – Manual download and installation
- Maintained via a commercial automated patching system

If Backup/Audits logs are not monitored it is possible that an anomaly may not addressed.

How to address/What is the Best Practice?

Monthly maintenance (patches, updates, cleaning, etc.) and monitoring plans should be identified for Hardware and Software. Inspection can be used to verify maintenance of updates.

Hardware and software needs maintenance to keep it secure and up to date. Operating systems (Windows, Mac OS, etc.), productivity software, web browsers all need regular “patching” and updating to fix vulnerabilities that have been reported. Most software security related updates are available for free from the vendor, but are not always automatically installed. These updates should be done on a monthly schedule by an assigned person.

For smaller networks (under 10 computers) a manual verification of the current version/update at each computer and the updating of computers and applications may be implemented.

For networks, greater than 10 computers, using an automated software to verify the current version/update at each computer and to perform the updating of computers and applications, also known as a commercial automated patching system. This would ensure the timeliness and accuracy of patches and application updates.

If you plan to handle IT support internally, you may want to purchase a commercial automated patching system, if outsourced support is used, software patching, automation of installation and monitoring should be included in your support agreement.

Audit logs (audit trail) should include - failed logins, user login, accessed/deleted files

Data Security – Encryption

What is it and its' application?

Encryption is the most effective way to achieve data security and should be used whenever possible. It is the process of encoding a message so that it can be read only by the sender and the intended recipient. Encryption systems often use two keys, a public key, available to anyone, and a private key that allows only the recipient to decode the message.

Transmission of personal/private information (or sensitive data) via the internet should be done over an https connection, protocol for secure communication. Web applications secure communication can be verified via an SSL certificate, or digital certificate that is installed on a web server and serves two functions:

- It authenticates the identity of the website (this guarantees visitors that they're not on a bogus site)
- It encrypts the data that's being transmitted

Email encryption can be implemented in several ways based on email protocol and data being sent:

- Message level – Entire message is encrypted
- Password protected file

Why is it important?

If a device is lost or stolen or data is intercepted encryption prevents unauthorized access by a third party without a password. Encryption should be used when any personal/private information is being transmitted via web applications or email.

How to address/What is the Best Practice?

Encryption is available on most common operating systems but is often not enabled by default however should be implemented on all municipal resources including computers, workstations, servers, laptops and mobile devices.

Annual review of encryption practices should be performed as the data transmitted changes and the protocol needs to align with needs. Encryption methods deteriorate as advances in technology occur; the review should verify coverage and strength and update to address deficiencies identified.

Data Security – Physical Security

What is it and its' application?

Physical security of Information Technology equipment can prevent unforeseen issues like theft or damage.

Why is it important?

Physical security of servers and network equipment is important to prevent data theft and equipment damage. Pets and unsupervised visitors can inadvertently cause damage to accessible equipment.

How to address/What is the Best Practice?

Servers, main network infrastructure, and data storage devices should all be placed in a secure location, ideally this would be in a climate controlled room, but a ventilated locked closet or storage cabinet could be sufficient.

The server and data should not be stored in an area that the general public has access to for theft prevention and reduces the risk of accidental damage.

Data Security – Remote Access

What is it and its' application?

Remote access is the ability to get access to a computer or a network from an alternate location; this is beneficial for telecommuters, and people who are travelling.

Why is it important?

Enabling remote access to an organization's network, systems and data can benefit most any organization however there are risks as well.

How to address/What is the Best Practice?

Remote access often requires additional technology investments for VPN (Virtual Private Network) security appliances and specialized firewalls to ensure privacy and add security to networks. Remote access creates additional security risks that must be carefully reviewed and monitored, particularly if the organization works with sensitive information or data.

Data Security – Data Compromise/Loss

Protecting data from unauthorized access, malicious or accidental deletion, data corruptions and physical security is one of the most important aspects of an IT plan.

What is it and its' application?

Data is always at risk for compromise, which can come in many forms:

- malicious - attacked via a virus, or a disgruntled employee
- a natural phenomenon
- an errant keystroke
- misrecorded information

Why is it important?

Data compromise or loss of irreplaceable records can be devastating for municipalities.

How to address/What is the Best Practice?

Ensuring that irreplaceable data has adequate Backup and Recovery, Data Storage or redundancy provisions and that the corresponding IT systems have adequate antivirus protection/alerting and access control.

A documented protocol and training with respect to Antivirus alert for users and administrators can aid in prevention of massive viral infections.

Data Security – Confidential Information

What is it and its' application?

Confidential Information is personal information beyond on Name and Address that can be gathered for employment or as a customer of the municipality. The confidential information needs to be controlled for privacy data breach to comply with security breach laws.

Why is it important?

Compliance with the Massachusetts security breach legislation is a requirement for municipalities.

How to address/What is the Best Practice?

Confidential information is defined as:

Name & Address* plus any of the following
Credit Card Information/Bank Account Numbers
Other Financial Information
Medical Records

Social Security Numbers Data Protection and Data Security measures should be applied to IT systems that handle confidential information.

Part III: Appendices

Appendix 1: Information Technology Policy

Information Technology Policy is the governing document, including the definition of hierarchy of documents and document definitions.

Hierarchy of documents and definitions:

1. Policy – protocol or guidelines
2. Procedure – specific method or official way (spreadsheets, forms, etc.)
3. Process – series of actions or steps

Any task identified in policy should have a corresponding procedure and process documented to ensure proper execution of the task.

Obligatory policy topics include but are not limited to:

- **Information Technology** (minimum requirement)
    - **IT Policies, Procedures and Processes** (minimum requirement)
- **Assets/Asset Management** (minimum requirement)
    - Operational requirements
        - Internet Connection
        - Mission Critical and Emergency Response
    - Hardware
    - Software
    - Inventory Data Collection
- Risk Assessment
- Legal/Regulatory Responsibility
- Device usage/restrictions (see BYOD)
- Access Control
    - User Logins
    - Passwords
    - Shared Logins
    - Additional aspects:
        - Internet
        - Email
        - Social Media
- Remote Access
- Security
- Employee Training
- Bring Your Own Device (BYOD)
- Maintenance and Monitoring
- Data Storage Plan

Appendix 2: Resource Tracking Record

Should include:

- Hardware or Software
- Asset Tag/ID
- Asset Type
- Date of purchase
- Installation date
- Ownership (responsible party)
- Location of Asset – storage and usage (i.e.: physical location, traveling resource assigned to First Last)
- Configuration
- Lifecycle
- 3 – 5-year plan*
- Replacement schedule information

*A replacement schedule should be considered when a new resource is appropriated.

Appendix 3: White and black lists

An application white list is the list of the only applications that are allowed to be installed and run.

- Any other application or program will be treated as a virus and not allowed to be run.
- This is the most secure option, but does require much more maintenance and support.
- The white list will need constant updates and modifications as business-critical applications are discovered and vetted.
- This type of setup is best for kiosk computers or other single task PCs.

Application black lists are the opposite of the white lists, all programs are allowed to be installed and to be run, except for the applications listed on the black list.

- This adds a level of security where known bad program can be blocked.
- Typical programs that are black listed are peer to peer file transfers, iTunes and other Apps stores, coupon printers and other browser toolbars, etc.
- This is the most common implementation of application management as it does not require as much up keep of the list and users are allowed to install software unless it is specifically blocked.

Appendix 4: Inventory data collection tool

Each inventory list should be maintained monthly and an annual audit should be part of the process to ensure accuracy.

For computers and workstations:

- Make
- Model
- Type (laptop, desktop, etc.)
- Serial number
- Amount of RAM
- CPU type and speed
- Hard drive space
- Optical Drive info
- Date purchased
- Date of warranty expiration
- Department/current location
- Date of assignment to current user
- Hostname
- Maintenance Log
- Upgrade Log

For network equipment: (Such as routers, firewalls and switches)

- Make
- Model
- Serial
- Type
- Hostname (if applicable)
- Date of purchase
- Date of installation
- Warranty or support expiration
- Current location

For software:

- Software Name
- Version
- Vendor Name
- Date Purchased
- Quantity (if VL or multi-user license)
- License info (key or agreement number)
- Where it is currently installed?
- Date it was installed

Appendix 5: Access Control Policy

User Logins

- Login credentials (with Password required) should be created for Users:
    - Unique User (a User Account) – named account i.e.: JohnSmith@
    - Do NOT create Shared logins – generic account (NOT recommended)
        - Password updates get overlooked
        - Login credentials are left in easily accessible places
        - Third party unauthorized access is easily accomplished
    - Role (a User Account) – i.e.: TownClerk@ versus named account
        - Ensures appropriate security settings
        - Enables continuity of information (historic and future access)
        - Departmental resource accessibility
- Permissions/Security settings should be defined and applied for each user with guidance.
- Network and data access is limited to data that is required to perform the duties of the User or Role.

User Accounts

User Accounts limiting access to network resources can be controlled via activation.

- Active: Limited access to network resources, only what is needed, based on security settings
- Inactive: Disable access to network resources.

i.e.: An intern User Account can be held inactive, to avoid the difficulty of access identification issues if they plan to return at a later date.

Passwords

- Passwords are used in combination with User Logins to gain access to data.
- Passwords prevent unauthorized third-party logins.
- Passwords prevent from external and internal attacks
- Passwords should be changed regularly and not shared with staff where possible.
- Passwords should meet a complexity standard and not be allowed to reused for a period of time.

The recommended complexity standard should be captured in a policy. This standard may not be supported by all programs designed for the end user, but attempt best effort to apply the rules in as many instances as possible.

- A common password policy would be:
    - 8 Character minimum
    - One Upper case letter
    - One lower case letter
    - One numeral
    - One special character (i.e.$#!@&*)
    - Expires every 90 days
    - Can't reuse last 3 passwords

Appendix 6: Procurement guidelines

- MGL Chapter 30B. Technology-related expenditures are subject to the state procurement law. The solicitation of three written quotes is required for purchases with a cost between $10,000 and $50,000. A purchase greater than $50,000 requires the town choose between soliciting sealed bids (IFB) or issuing a Request for Proposals (RFP). RFPs may only be issued by the Town's Chief Procurement Officer (CPO).
- State Bid List. The town should also research the Commonwealth Statewide Contract System (CommBUYS). Managed by the Commonwealth's Operational Services Division (OSD), CommBUYS is a clearinghouse of public procurement opportunities for awarding authorities and companies interested in doing business with state and local governments. Municipalities can, at no cost, publish any bid requests, making them available for review by prospective bidders. This saves a municipality the cost of bidding although towns are required to solicit quotes under the CommBUYS system in many cases. The town should also be aware that the State bid list tends to offer greater hardware, than software, selections.
- Financing. The town has options for software and hardware purchases.
  - a. *Available funds*. Free Cash, General Stabilization Fund, Special Purpose Stabilization Funds and Special Revenue Funds all represent potential pools of money that can be used for technology purchases. Use of these funds do not impact the property tax rate, but must be approved by a Town Meeting vote.
  - *b.* *Excess Levy Capacity*. The difference between the total tax revenue a town is permitted to collect under Proposition 2 ½ and the amount it actually chooses to collect is Excess Levy Capacity. The current year Excess Levy Capacity approximates available tax revenue in the next year that can be raised to fund capital purchases or projects as a direct dollar outlay, or to pay annual debt service on capital investment funded through borrowing. In all cases, the use of Excess Levy Capacity results in a property tax increase.
  - c. *Borrowing within the Town Levy*. Town Meeting always has the option of authorizing the issuance of notes, bonds or a combination of both to fund technology purchases. (MGL Ch. 44, §7, cl. (28) or (29)) Borrowing within the Levy means that the town has the capacity to pay issuance costs and debt service within the annual budget without imposing a property tax increase.
  - d. *Borrowing with a Debt Exclusion*. When Town Meeting approves a borrowing authorization to fund a technology purchase, it can attach a Debt Exclusion. This is a means to raise tax revenue, above and beyond Proposition 2½ limits, to pay debt service on the borrowing. The tax increase remains only for as long as the borrowing term and requires approvals of both a two-thirds Town Meeting vote and a majority town wide ballot vote.
  - e. *Capital Expenditure Outlay Exclusion*. Under Proposition 2½ (M.G.L. C. 59, §21C7, clause j), a capital exclusion enables the town to raise additional tax revenue, in one year only, to cover

the entire amount needed to pay a software and/or hardware cost. Town Meeting must approve the appropriation citing a capital exclusion as the funding source. The Select Board must place the capital exclusion question on a town ballot for resident approval by a majority vote.

Appendix 7: Town of Conway IT Best Practices Policy Statements

In an effort to comply with best practices for municipalities it is recommended that all municipalities meet or exceed the following guidelines:

NOTE: “The municipality” can be directly substituted with the name, ie: Town of Conway

Fundamentals of an IT system

Internet Connection

The municipality will implement an Internet Connection with a constant high-speed connection that provides access to email, software updates and other critical services, such as web based applications.

File Backup

The municipality will implement a regularly scheduled file backup of all critical data.

Strong Passwords

The municipality will implement formal rules for password format and usage including changes, duplication and protection.

Anti-Virus (Licensed) on all Computers

The municipality will implement paid antivirus options licensed for Commercial or Government use on all computers.

Computers running up to date (vendor supported) software

The municipality will implement a software update program to ensure proactive downloading and installation of software updates for the current version (not version upgrade) regularly or are automated for each software application (Operating system, browser, third party software, etc.).

Annual IT Evaluation

Based on the Annual IT Evaluation Checklist the following Policy Statements can assist in implementation of IT Best Practices

Section 1, Annual IT Evaluation: Asset Management Assessment

1.1 The municipality will implement an accurate detailed inventory of hardware.

1.2 The municipality will implement an accurate detailed inventory of software.

1.3 The municipality will implement a scheduled/periodic review of hardware and software to update the inventory.

1.4 The municipality will implement a hardware replacement schedule.

1.5 The municipality will implement a software replacement/upgrade schedule in place? (General - MS Office, departmental level (SoftRight, VADAR, Point)).

1.6 The municipality will implement central oversight of IT expenditures.

1.7 The municipality will implement an established protocol for annual IT expenditures, whether through the operating budget or capital budget.

Section 2, Annual IT Evaluation: Data Security

2.1 The municipality will implement awareness of confidential information stored on the IT system and ensure proper handling.

2.2 The municipality will implement authorization & control measures for Town owned Confidential information stored on electronic devices (i.e. laptop, cell phone, tablet, etc.) that is permitted to be removed from municipality premises.

2.3 The municipality will implement a program to ensure permitted authorized remote access to the town network and town computers.

2.4 The municipality will implement proper measure if it accepts credit cards for bill payments.

2.4.1 The municipality will implement data and system protection agreements with any third party that accepts credit card payments on behalf of the town.

2.5 The municipality will implement a process for assigning staff permission levels that allows or restricts access to electronic data.

2.6 The municipality will identify known deficiencies in the security practices of the municipality.

If deficiencies are identified, please detail the deficiencies and resolution on a separate sheet

2.6.1 The municipality will implement a procedure to record and resolve known deficiencies in the security practices of the municipality.

2.7 The municipality will implement that all users with access to systems are authenticated by means of unique and individually assigned passwords, physical characteristics or digital ID.

2.8 The municipality will implement control of network and data access by role based user authentication rather than name based user authentication.

2.9 The municipality will implement procedures to ensure the proper use of file sharing or Peer to Peer networking technology if allowed.

2.10 The municipality will implement secure storage areas (i.e. locked rooms, locked file cabinets, limited access areas, etc.) for documents containing customer and/or employee personal identification information.

2.11 The municipality will implement identify a person or party to determine the municipality risk tolerance levels?

Section 3, Annual IT Evaluation: Monitoring and Maintenance

3.1 The municipality will implement an established relationship with an external IT professional or IT firm to provide ongoing and emergency technical support.

3.2 The municipality will implement protocols or steps the staff are directed to take, in the event of a data breach.

3.3 The municipality will implement and maintain an audit trail that documents user activity (passwords and permissions).

3.4 The municipality will implement Firewalls, Spam Filters, Virus Protection etc. and updated them at least quarterly.

3.5 The municipality will implement a scheduled/periodic review of software updates and patches.

3.6 The municipality will implement secure email practices (i.e. automatically scan & filter emails).

3.7 The municipality will implement a Network intrusion detection sensor alert?

3.7.1 The municipality will implement a protocol for a Network intrusion detection sensor alert.

3.8 The municipality will implement an Antivirus software alert?

3.8.1 The municipality will implement a protocol for an Antivirus software alert.

3.9 The municipality will implement an alert for multiple failed login attempts?

3.9.1 The municipality will implement a protocol for multiple failed login attempts alert.

Section 4, Annual IT Evaluation: Data Backup

4.1 The municipality will implement and adhere to a written data back-up plan.

4.2 The municipality will implement a written data disaster recovery plan.

4.2.1 The municipality will ensure a written data disaster recovery plan is tested through a simulation or exercise.

4.3 The municipality will implement programs to back-up network data and configuration of files daily.

Section 5, Annual IT Evaluation: Regulatory Responsibilities

5.1 The municipality will implement a program to ensure a specific data retention/destruction schedule is adhered to, in compliance with MA Public Records law.

5.2 The municipality will implement procedures to ensure its service providers to maintain at least the same level of data security regimen that it maintains.

5.3 "The municipality will implement a procedure to ensure the Treasurer, TA, and other responsible parties are aware of their regulatory responsibilities

For example: Ambulance, Fire, etc."

Part IV: Glossary

Glossary of Terms	Sources: http://whatis.techtarget.com/ and http://www.gartner.com/it-glossary/	
Term	**Definition**	**Prevention Method**
Adware	A software application in which advertising banners are displayed while the program is running; sometimes, also tracks user information, which makes it also spyware.	see Spyware
Antivirus Software	Antivirus (anti-virus) software is a class of program that will prevent, detect and remediate malware infections on individual computing devices and IT systems.	N/A
Bring Your Own Device (BYOD)	see BYOD	N/A
Business Continuance (Continuity)	Business continuance is a strategy for putting the processes and procedures in place that an organization requires to operate during and after a disaster. Business continuance plans seek to prevent mission-critical services from being interrupted and re-establish full operations as swiftly and smoothly as possible.	N/A

Term	Definition	Prevention Method
BYOD	Bring your own device (BYOD) is an alternative strategy allowing employees, business partners and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data. Typically, it spans smartphones and tablets, but the strategy may also be used for PCs. It may include a subsidy.	N/A
Confidential Information	Name & Address* plus any of the following Credit Card Information/Bank Account Numbers Other Financial Information Medical Records	Data Security – Confidential Information
Device	Typically, a Smartphone/tablet however in some cases a laptop or PC.	N/A
E-mail Virus	Malicious computer code (malware) sent to you as an e-mail attachment.	The best two defenses against e-mail viruses for the individual user are (1) a policy of never opening an e-mail attachment (even from someone you know) unless you have been expecting the attachment and know what it contains, and (2) installing and using anti-virus software to scan any attachment before you open it.
Emergency Response	Response to computer security incidents, report on vulnerabilities and promote effective IT security practices	N/A

Term	**Definition**	**Prevention Method**
Executable	Type of file containing a program that will start it to run; viruses are often sent in executable files that will run when the user opens the file.	N/A
File Sharing	The public or private sharing of computer data or space in a network with various levels of access privilege (i.e.: 3rd party, dropbox).	N/A
Firewall	A firewall is an application or an entire computer (e.g., an Internet gateway server) that controls access to the network and monitors the flow of network traffic. A firewall can screen and keep out unwanted network traffic and ward off outside intrusion into a private network. This is particularly important when a local network connects to the Internet. Firewalls have become critical applications as use of the Internet has increased.	N/A
Hardware	The physical aspect of computers, telecommunications, and other devices. I.e.: Computers, servers, switches, printers, etc.	N/A
Infrastructure	Computer resources, complemented by storage and networking capabilities are owned and hosted by a service provider. The construction, design, and use of a network, including the physical (cabling, hub, bridge, switch, router, and so forth), the selection and use of telecommunication protocol and computer software for using and managing the network, and the establishment of operation policies and procedures related to the network	N/A

Term	Definition	Prevention Method
IT resources	Physical Information Technology equipment and the plans, budgets, actions, procedures, documents (It includes, but is not limited to Computers, monitors, servers, software/hardware, networks, switches, components, procedures, services, etc.).	N/A
IT System	A computer or set of computers, servers, devices used to create, process, store and distribute information	N/A
Malware	Programming or files developed for the purpose of doing harm. All-encompassing title - adware, pop-up, redirection, spyware, virus	Computer Use Policy
Mission Critical	Any information technology (IT) system or network device whose loss would cause business operations to fail	Is internet a requirement? Is the server the data warehouse? Does the device control a shared resource?
Network	Infrastructure - Wired or Wireless Minimum pieces to be a network: A firewall, a router (switch) creating interconnectivity to share a resource (i.e.: internet) between at least 2 devices (a computer and ?)	N/A
Patch	A quick-repair job for a piece of programming, often as a result of some discovered vulnerability.	N/A
Peer-to-peer (P2P)	Style of networking in which computers communicate directly with one another rather than routing traffic through managed central servers and networks.	N/A

Term	Definition	Prevention Method
Risk mitigation	Identify, manage and mitigate IT and enterprise compliance risk	N/A
Risk prevention		N/A
Router	In packet-switched networks such as the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination.	N/A
Security update		N/A
Server	A type of computing appliance that creates, manipulates or provides information to other network-connected computing devices. Unlike storage appliances, server appliances use an application context for the creation, manipulation or provision of information.	N/A
Service Provider	Organization providing a service to the municipality, not limited to only IT service provider, can be ISP, telecom, banking, etc.	N/A
Social Engineering	A non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.	Awareness
Software	A general term for the various kinds of programs used to operate computers and related devices.	N/A

Term	**Definition**	**Prevention Method**
Spyware	Spyware is software that is installed on a computing device without the end user's knowledge, can be tracking software to secretly gather information about the user and relay it to interested parties.	To prevent spyware, users should only download software from trusted sources, read all disclosures when installing software, avoid clicking on pop-up ads and stay current with updates and patches for browser, operating system and application software.
Switch	see Router	N/A
System Management	Any of a number of “housekeeping” activities intended to preserve, maintain or correct the operation of a computer system. Included are such routine but critical processes as hardware diagnostics, software distribution, backup and recovery, file and disk integrity checking, and **virus** scanning.	N/A
Virus	A piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A virus is often designed so that it is automatically spread to other computer users. Generally, there are three main classes of viruses: file infectors, system or boot infectors, and macro viruses.	The best protection against a virus is to know the origin of each program or file you load into your computer or open from your e-mail program. Since this is difficult, you can buy anti-virus software that can screen e-mail attachments and also check all of your files periodically and remove any viruses that are found.