



BAINBRIDGE ISLAND FIRE DEPARTMENT



**Information Technology Plan
Effective: 10/07/2020**

TABLE OF CONTENTS

Chapter 1 - Introduction	2
Chapter 2 - Vision	3
Chapter 3 - Purpose	3
Chapter 4 - Current Environment	4
Chapter 5 - Goals / Objectives / Initiatives	6
Communication & Collaboration	6
IT Infrastructure	7
Information & Document Management	9
Digital Identity Management & Cybersecurity	9
Prioritization & Funding of Information Technology	9
Department-Wide IT Familiarization/Training	10
IT Management Structure	10
Chapter 6 - Estimated Timelines & Costs	10
Chapter 7 - Glossary (or List of Acronyms)	11



INTRODUCTION

1

The impetus for the following document stems from the *Information Technology* chapter of the Bainbridge Island Fire Department 2019-2024 Strategic Plan (the Strategic Plan), wherein three strategic goals were summarized as follows:

1. Develop a comprehensive Department IT Plan (subsequently identified as *IT Master Plan* on the Department's 2020 Work Plan, as approved by the Department's Board of Commissioners on January 21, 2020).
2. Establish an IT equipment replacement schedule.
3. Maintain cybersecurity with all electronic communications.

Upon approval by the Department's Board of Commissioners, this document represents the accomplishment of the first strategic goal identified above. The second and third goals from above have been restated and incorporated within this document.

In accordance with the Department's *Policy & Procedure #124-Committees*, Fire Chief Hank Teran authorized and convened an IT Committee on May 20, 2020, comprised of the following members: Tim Carey (appointed as chairperson), Hilary Hall, Ed Kaufman, Dag Liljequist, Jeffrey Milsten, Jared Moravec, Jackie Purviance, Chris Schmit, and Fritz von Ibsch. Chief Teran identified the Committee's objective as to provide for his consideration a written form of innovative IT recommendations and advice, designed to both guide Department-level decision-making and budgeting, and to perhaps influence similar County-level activity.



Compassion

Trust

Stewardship

Innovation

Courage

BIFD Core Values

Committee members respectfully submit the following work product (the IT Plan) as the result of twenty-one videoconference meetings over the course of nearly five months during the COVID-19 pandemic. The format is intentionally succinct, yet packed with the results of deliberate, thoughtful, and collaborative discussion. Importantly, this IT Plan is intended to be subservient to the Strategic Plan in that if any subsequent revision of the Strategic Plan identifies divergent strategy from the existing IT Plan, the Strategic Plan shall prevail.



VISION

2

This Plan's vision is to provide innovative, value-oriented, secure, reliable, and integrated technology solutions, which allow effective and efficient internal and external departmental data transfer and communications.

PURPOSE

3

This Plan shall guide the Department's IT direction, alignment, investments, and accountability of its members, in support of the Strategic Plan. It is conceived with a three to five year horizon and assumes future updates as needed to support future iterations of the Department's strategic planning efforts. The guidance provided by this Plan is intended to nurture efficient and effective work processes, service delivery, and communications. It takes into account current IT needs, and to the extent possible, provides a forecast of future needs. It is intentionally broad-focused to allow flexibility in tactical implementation.

CURRENT ENVIRONMENT

4

“Information technologies have become an integral and indispensable component of the Department’s daily activities, so much so that it is important to prioritize IT in all future planning. Today, the Department uses technology for such diverse applications as incident response, building inspection, hydrant inspection, public outreach, training, emergency preparedness, and more. IT permeates every facet of the Department’s mission.

The past 10 years have seen tremendous change in the way the Department responds to calls, processes incidents, communicates with its partner organizations, and completes reports detailing each event. Gone are the days of manually handwriting medical incident reports. Reporting of incident responses now include real-time entering of data and transmitting that data immediately to destination hospitals to facilitate faster and more complete patient care”.

- From the Strategic Plan -



In the above quote, the Strategic Plan capably summarized the Department’s IT environment in 2019. With the Department’s existing IT infrastructure beginning to age, with information and communication technology changing rapidly, and with the needs of citizens and Department staff developing as rapidly, assembling an IT Plan had become an organizational priority.

Since then, and as a result of this Committee’s impressions, research, and analysis, it became clear that the following additional factors (while perhaps not an exhaustive list) justify both the need for, as well as the content within, this IT Plan:

- 1) The way fire departments serve and interact with citizens, businesses, neighboring districts, hospitals, and other groups is changing; IT plays a pivotal role in those changes.
- 2) This is an exciting and challenging time in which technology is both driving and being driven by changes in the way people live their lives and share information. Especially with consideration of the current worldwide pandemic, wireless technology, social networking, and teleconferencing, to name just a few, are creating new challenges and opportunities.



- 3) Smartphones and mobile computing are becoming dominant forces. The majority of Web pages viewed is through these devices. It is incumbent on fire departments to adapt to this paradigm shift and offer smartphone and mobile device-friendly access to information through the Web and other applications.
- 4) There is an increasing need for organization-wide (“enterprise”) IT solutions that are integrated to improve the way the Department serves citizens and businesses.
- 5) Many larger technology infrastructure improvements are long-term investments and require careful planning and research before they are implemented.
- 6) The role of IT support will need to expand to include not only expert care of the IT infrastructure and applications, but also to take on a more proactive consulting, facilitating and leadership role. This new role involves understanding and interpreting needs, communicating IT needs and possibilities, developing and improving business processes, and finding and coordinating appropriate solutions.



- 7) Users will need to be more proactive and timely in communicating their needs, desires and new developments in technology in their disciplines to those in charge of IT support. IT support will need to play a more consultative role across the Department’s Organizational Chart to facilitate two-way and multi-way communication among stakeholders.
- 8) Technology is changing rapidly, and many technologies that may be in use in five years have not been developed or even invented.
- 9) In these challenging economic times, IT departments are embracing Cloud-based, open source and virtual solutions. It appears these shifts will continue well into the future and will be long-lasting.



- 10) Over the past 10 years, ongoing maintenance costs have been consuming an ever-larger share of IT budgets. As the IT industry shifts to the Cloud and other application service provider models, recurring costs will be an even greater portion of budgets, although there may be savings in capital costs associated with these technologies.
- 11) It is advantageous to seek out and deploy technology that adheres to open, vendor-independent standards, and to minimize proprietary solutions.
- 12) Cyber attacks are growing in number and in sophistication; proactively protecting the Department's information technologies is critical.
- 13) As employees are being asked to do more with the same resources, it is critical that the Department provides them with the IT tools they need to do their jobs.
- 14) Mergers and acquisitions of technology companies, including those providing products and services to local fire departments, significantly result in less competition, fewer choices of products and rising prices.
- 15) Department processes, regulations and audit requirements do not always support flexibility, quick changes or selecting the most-favored new technology.
- 16) The needs and desires of staff, and the public, as well as the way they use technology, are increasing and changing, sometimes at different rates.
- 17) In employing IT solutions, it can be difficult to balance proven versus leading-edge technology.

GOALS / OBJECTIVES / INITIATIVES

5

1. Goal: Communication & Collaboration

a. Objective: Video conferencing

- i. Initiative: Review video-conferencing solution as it pertains to delivering instructor-led training from a central location, ensuring video/audio quality for all participants.



- ii. Initiative: Define the need/cost/feasibility for video-conferencing in spaces within each station in terms of how each space is to be used (i.e. FS 21’s public meeting room could be set up to allow streaming content to the public and/or Commissioners, and FS 23’s Training Room could be set up to allow streaming content needed for Backup EOC).
- iii. Initiative: Replace Department-issued laptops deemed insufficient for video calls with respect to both image and audio quality, based on an objective written requirements list.



b. Objective: Audio

- i. Initiative: Conduct Department-wide needs assessment of the physical phone systems, with the intent of likely replacing all phone systems at all stations, taking into account conference rooms, teleworkers, and public spaces potentially needing remote microphones, and redundancy (spare phones and spare parts) throughout.
- ii. Initiative: Conduct Department-wide needs assessment of analog phone lines to determine for what purpose we are currently using them and document scenarios in which we may need them (i.e. natural disasters, power failures, elevator).
- iii. Initiative: Conduct needs assessment of digital phone lines vendor with respect to redundancy and single points of failure.

c. Objective: Messaging (all kinds)

- i. Initiative: Define scope of use and permissions necessary to promote use of teams-based software (i.e. MS Teams) as the collaboration platform to serve all areas of the Department’s Organizational Chart. 
- ii. Initiative: Develop “messaging use-case scenarios” for both Department-issued and personal devices, and evaluate which messaging platforms (i.e. SMS text, MMS text, Apple Messenger, Microsoft Teams chat, etc.) are compatible with Department records retention policies in terms of fulfilling public records requests.

2. Goal: IT Infrastructure (Increase and enhance effective and efficient delivery of integrated quality services for internal and external uses).

a. Objective: Fixed network infrastructure

- i. Initiative: Define and implement identified redundancy needs as they relate to internet access.



b. Objective: Mobile network infrastructure (vehicles) - WIFI to LTE connection

- i. Initiative: Define and implement identified redundancy needs as they relate to mobile internet access (i.e. review the use of the Pepwaves and consider dual SIM-Card solutions for mobile devices).

c. Objective: Mobile device management

- i. Initiative: Research and deploy Cloud-based software centralizing management of mobile devices (cell phones, laptops, tablets, desktop PCs) from initial deployment to retirement, including “zero-touch provisioning” with pre-approved/installed software.

- ii. Initiative: Prioritize Wi-Fi connections to ensure devices are connected to the correct Wi-Fi signal (i.e. MCT’s or perhaps LifePaks or other devices shouldn’t switch Wi-Fi connections from rig to station upon returning from a call).

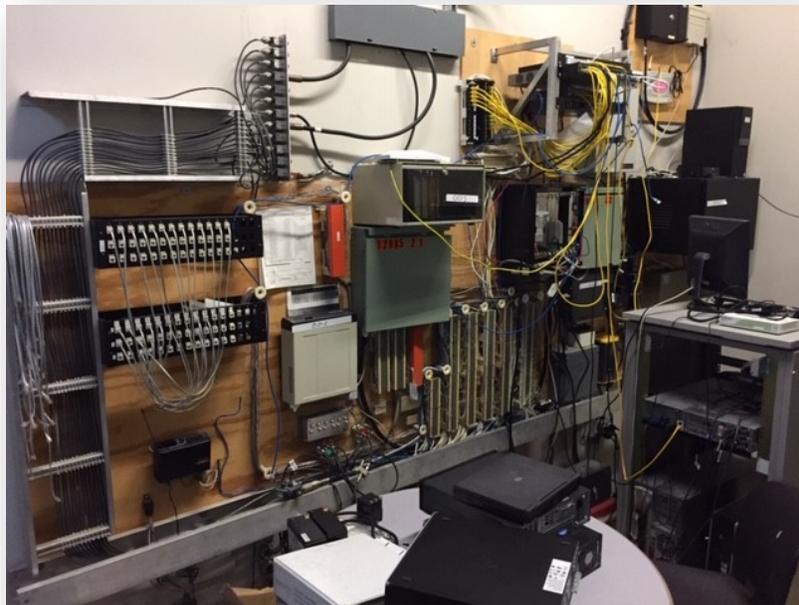


d. Objective: Monitoring (i.e. MCT’s, tablets, cell phones, Lifepacks via Pepwaves, and Knox Boxes)

- i. Initiative: Assess the effort required to monitor all systems, both internal and external (i.e. Internet, Pepwaves, phone lines, VOIP lines, station alerting system, CAD-link) used by the Department and determine if building a dashboard makes sense.

e. Objective: Cloud solutions/physical servers

- i. Initiative: Assess current and projected server needs both on premises and Cloud-based.





3. Goal: Information & Document Management

a. Objective: Enhance data & document storage, retrieval, organization, sharing and access

- i. Initiative: Design and implement SharePoint structure for easy storage/retrieval (needs to take into account public records requests, as well as the Department's internal needs).

b. Objective: Use data to improve analysis and decision-making

- i. Initiative: Continue to utilize data analysis tools like Tableau to enrich understanding of data-driven decisions.

4. Goal: Digital Identity Management & Cybersecurity

a. Objective: Employ, where possible, Digital Identity Management - Single Sign On

- i. Initiative: Evaluate the implementation of SSO with each Cloud-based solution used by the Department.
- ii. Initiative: Add SSO as a requirement of acquisition of any new Cloud-based solution.

b. Objective: Security

- i. Initiative: Evaluate multi-factor authentication.
- ii. Initiative: Evaluate machine-to-machine authentication (i.e. MCT's authenticating via VPN to a server at Kitsap 911).
- iii. Initiative: Evaluate use of any remaining shared passwords.



5. Goal: Prioritization & Funding of Information Technology

a. Objective: Develop Department-wide best practices for prioritizing and funding IT solutions and projects

- i. Initiative: Identify criteria for objective evaluation of IT spending in advance of annual budgeting process.
- ii. Initiative: Evaluate the need for a separate IT Cost Center within Department Budget, taking into account expenses related to Cloud-based software, on-premise software, software support, hardware, etc.
- iii. Initiative: Expand IT section of 10-year financial plan for enhanced long-term budget projections.
- iv. Initiative: Develop device replacement plan that includes a schedule for physical replacement, projected expenses, and defines buying criteria (i.e. considerations of user needs and minimum specifications).



6. Goal: Department-Wide IT Familiarization/Training

a. Objective: Increase technical proficiency and expertise

- i. Initiative: Assess the degree and scope of training curriculum needed to increase Department members' technical proficiency and expertise across all software and hardware.

7. Goal: IT Management Structure

a. Objective: IT support delivery

- i. Initiative: Assess/Determine/Justify/Recommend use of an outside consultant service versus an in-house IT staff and/or the balance in scope-of-work between such service providers.
- ii. Initiative: Maintain an IT inventory, which tracks criteria deemed necessary by the Department beyond the small and attractive assets provisions already required by the State Auditor.

b. Objective: Efficiently manage software solutions and licensing

- i. Initiative: Assess overlaps in software solutions and reduce overlap to the extent possible (ERS, ESO, Target Solutions, etc.).

ESTIMATED TIMELINES & COSTS



Initiatives identified in this document are best prioritized and scheduled in concert with the Department's Annual Work Plan.



GLOSSARY (OR LIST OF ACRONYMS)

7

Apple Messages: An instant messenger service that allows end users to send texts, documents, photos, videos, locations, contact information and group messages over Wi-Fi, 3G or LTE networks to other iOS or OS X users.

CAD-Link: Computer-Aided Dispatch link between the Department and Kitsap 911.

Cloud: Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet.

ERS: Emergency Reporting System - an online, subscription-based records management tool used for incident reporting, inspections, maintenance, and other Department programs.

ESO: Online, subscription-based patient care reporting system mandated by the Medical Program Director.

IT: Information Technology - the use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.

LTE: Long-Term Evolution - applies more generally to the idea of improving wireless broadband speeds to meet increasing demand.

MCT: Mobile Computer Terminal - computers mounted in apparatus to communicate back with Kitsap 911.

MDM: Mobile Device Management - an industry term for the administration of mobile devices, such as smartphones, tablet computers and laptops. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices.

MFA: Multifactor Authentication - multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence. Two-factor authentication is a type, or subset, of multi-factor authentication.

Microsoft Teams Chat: Microsoft Teams is a unified communication and collaboration platform that combines persistent workplace chat, video meetings, file storage, and application integration.

MMS Text: Multimedia Message Service - a system of communication whereby devices can communicate in a more sophisticated way than SMS Text, including pictures and other multimedia elements.



Mobile Hotspot: A handheld wireless router for providing Internet access to nearby devices via cellular.

Pepwave: Essentially a wireless router on each rig (peplink.com) connecting to the Internet via cellular.

SIP Phone Lines: Digital phone lines that provide dial tone over the Internet/fiber.

SMS Text: Short Message Service - a system of communication whereby devices can communicate simple, short messages.

SSO: Single Sign On - an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. It is often accomplished by using the Lightweight Directory Access Protocol and stored LDAP databases on servers.

Target Solutions: An online, subscription-based training management platform.

VPN: Virtual Private Network - a secure network connection that is encrypted between the device and server.