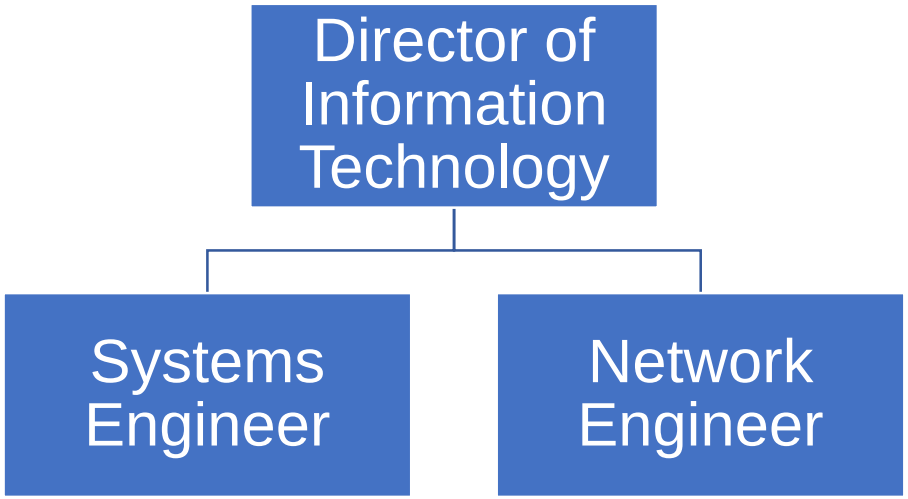
INFORMATION TECHNOLOGY DEPARTMENT

2020 Budget Presentation

Information Technology Department

Organizational Chart



Full-Time Equivalents: 3

Vision: Drive necessary and effective IT capabilities for improved operations and collaboration across the City

Mission: Create an interconnected and informed City through the prioritized, secure, and innovative application of IT resources.

Department Responsibilities:

- Desktop Support
- Systems
- Infrastructure
- Telecommunication
- Cyber Security
- Project Management

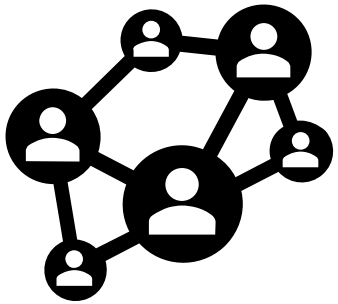
CITY OF Saco
www.SacoMaine.org

IT Major Functions

- Governance

- Infrastructure

- Functionality



CITY OF Saco

www.SacoMaine.org

Major Accomplishments

- Server migrations – IMC, Vision, email, Munis, WatchGuard
- Collaboration efforts – SharePoint, O365
- Enhanced City Wi-Fi capabilities
- Mobile Device Management
- Expanded wire infrastructure
- Project plan to migrate to a hyper-converged infrastructure
- Spear Phishing and Phishing campaigns

CITY OF Saco
www.SacoMaine.org

Major Accomplishments

- Tested: New backup software, Anti-virus, security applications
- Identified security vulnerabilities
- Built out City of Saco Cyber Incident Response Kit
  - Includes step by step guide to initial response, imaging, analyzing, and reporting
- Replaced all City copiers and printers
- Held user trainings which included:
  - Senior Security Training, Employee Security Training, SharePoint, and Outlook

Vendors

DOSSIER SYSTEMS

gwi Phone, Internet & Beyond

Microsoft Office 365

DigitalSky ONE COMPANY. ONE NUMBER. TOTAL SOLUTION™

spiceworks

FORTINET

KnowBe4 Human error. Conquered.

VISION GOVERNMENT SOLUTIONS

iWorQ

DELL

WATCH GUARD

CENTRALSQUARE TECHNOLOGIES

revize. The Government Website Experts

CITY OF Saco

www.SacoMaine.org

RAD FY2019 Update

- Blank-it: We decided that this product was not the best solution we would get to achieve the desired function.

- I-Worq: Adding additional modules – online permitting, planning, and licensing should be fully implemented by the end of the FY

- Nessus: Amazing capabilities, identified many vulnerabilities in the City of Saco network.

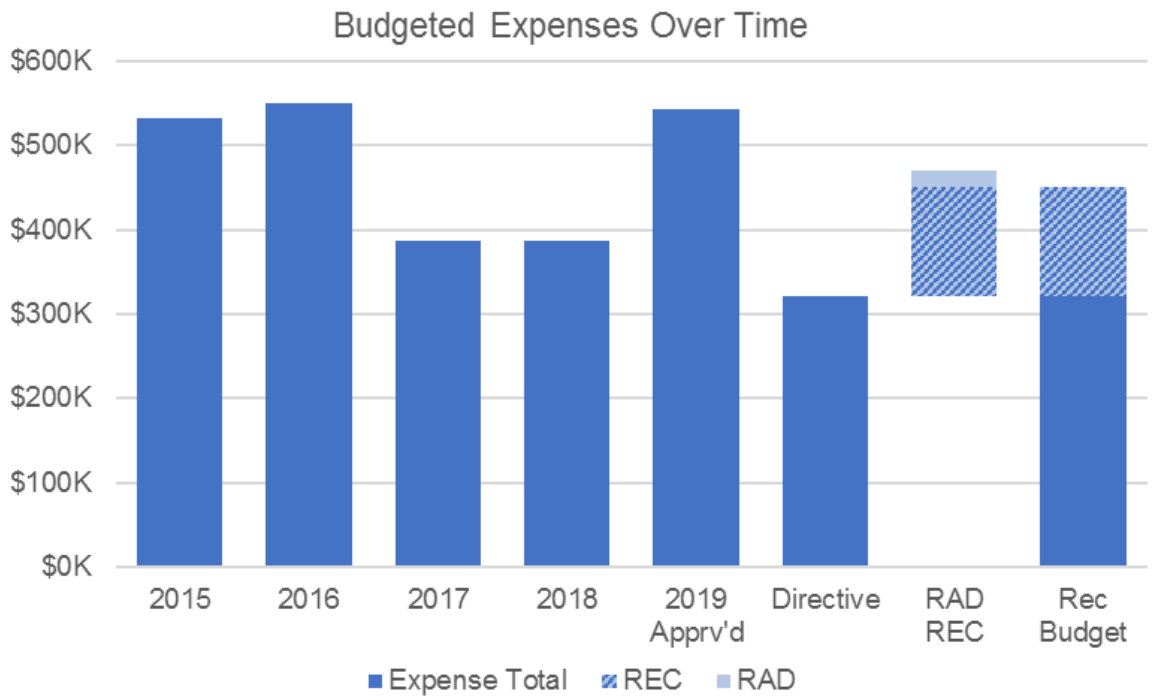
CITY OF Saco
www.SacoMaine.org

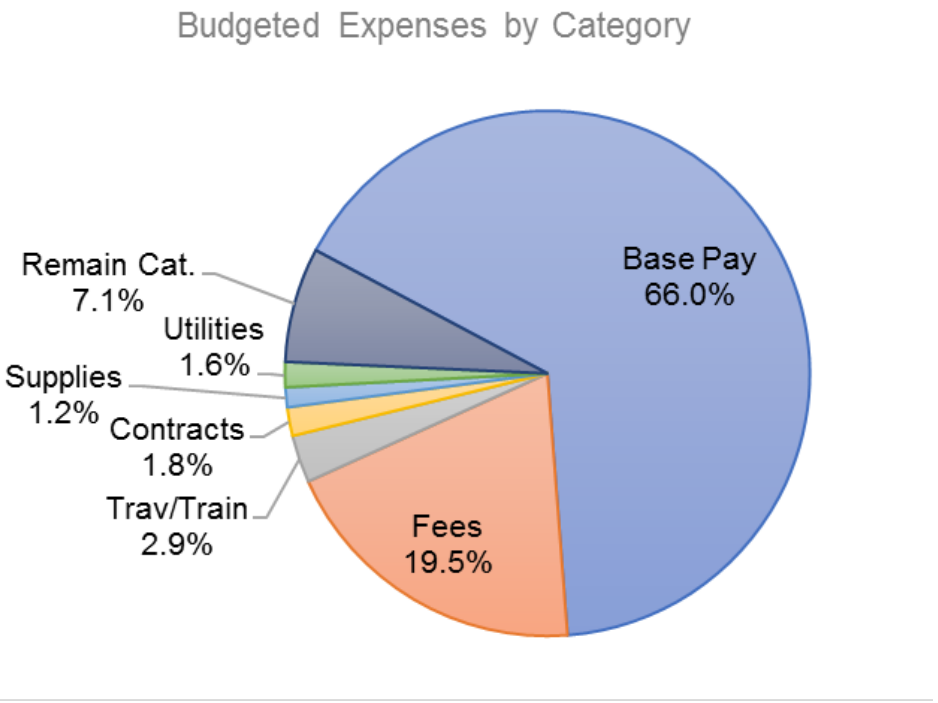
Major Challenges

- Security threats
- Innovation and digital transformation
- Interoperability
- Balancing security and accessibility
- Merging old with new

CITY OF Saco
www.SacoMaine.org

Budget Summary





CITY OF Saco
www.SacoMaine.org

Budget Summary

	FY2019 Adopted	$ Change	FY2020 Directive	RADs	REC RADs	FY2020 Recommended
Expense	543,871	(222,941)	320,930	148,779	130,458	451,388
Revenue	0	0	0	0	0	0
Operating Income	(543,871)	222,941	(320,930)	(148,779)	(130,458)	(451,388)

CITY OF Saco
www.SacoMaine.org

Requests Above the Directive

	Project Name	Priority	Frequency	Requested	Recommended
	Additional Email Licenses	**Critical Need**	Ongoing	11,020	0
	Additional Email Licenses Total			**11,020**	**0**
	Cyber Security Program Manager	**Critical Need**	One-Time	5,805	5,805
	Cyber Security Program Manager		Ongoing	115,822	115,822
	Cyber Security Program Manager Total			**121,627**	**121,627**
	Sophos Intercept X + EDR	**Critical Need**	Ongoing	13,500	13,500
	Sophos Intercept X + EDR Total			**13,500**	**13,500**
	nDiscovery - Managed Threat Protection	**Critical Need**	Ongoing	10,000	10,000
	nDiscovery - Managed Threat Protection Total			**10,000**	**10,000**
Grand Total				**156,147**	**145,127**

CITY OF Saco

www.SacoMaine.org

Cyber Security Program Manager

- Request: The time it takes to deal with all the security threats we face has become daunting. This position will be devoted to ensuring the City of Saco maintains a minimal threat vector and create a secure working environment for users and the public.
- Expense:
  - Salary – Ongoing – 115,882
  - Equipment – One-time(ish) - 5805
    - Includes – Laptop, initial licensing, desk, chair

CITY OF Saco
www.SacoMaine.org

Cyber Security Program Manager – Task List

Email & Web Sec	MFA	IDS/IPS	Security Patching	Endpoint Protection
Account review	ACL	Encryption	Policies	Sec Training
Inventory	Review FW, VPN	Network doc	Monitoring	Incident Response
Secure File Xfer	Reporting	Risk Assessment	Vul Testing	Pen Testing
SIEM	MDR	PCI Compliance	Risk Management	Vul Management
Mobile	NAC	DLP	ID Access	Forensic Cap
Application Testing	Info Governance	CJIS Compliance	PCI Compliance	Log Management

CITY OF Saco
www.SacoMaine.org

Cyber Security Program Manager

- Is the threat really present?
  - Yes, ~30 attempts on boundry protection daily
  - Yes, ~15 attempts to send malicious emails to users
  - Yes, ~40k attempts to brute force into now disabled RDP
  - Yes, while users are a huge vulnerability we cannot expect users to be human firewalls. We can train them the best we can, however, everyday a new zero-day is created and it would be impossible to ensure users are constantly aware of the current threats.
  - Yes, Albany, NY – Atlanta, GA – Rockport, ME – Spring Hill, TN – Saco, ME

CITY OF Saco
www.SacoMaine.org

nDiscovery

- Request: The City of Saco IT team has identified the need for 24/7 threat analysis, and management. Sage Data Security is a Maine based company that can provide this service.
- Expense: 10,000

CITY OF Saco
www.SacoMaine.org

nDiscovery

- What is nDiscovery?
  - Contextual & Behavioral analysis
    - Examination of behavioral attributes – Detection of sophisticated and zero day threats
  - Current Threat Intelligence
    - Up-to-date and on-going security analysis and intelligence from public and private data repositories
  - Data Aggregation & Advanced Analytics
    - Remove silo and gain insight to detect new threats before automated tools know they exist
  - Business-Specific Context & Security Intel
    - Develop baseline behavior, intel based on type and applied from all

CITY OF Saco
www.SacoMaine.org

Sophos Intercept X with EDR

- Request: Replace existing AV with a more advanced and easier to manage system. Our current AV is clunky, and is time consuming when changes need to be made. With Sophos Central we are able to make changes quickly with a much easier to use GUI
- Expense:
  - Users Central - 2300/year + Intercept X 3300/year + EDR 5500/year
  - Servers Central - 470/year + Intercept X 1000/year + EDR 900/year

CITY OF Saco
www.SacoMaine.org

Sophos Intercept X with EDR

- Sophos Central – central portal
- Intercept X – Deep learning malware detection
- EDR – Endpoint detection and response
  - Gives us the ability to detect, investigate, and respond
  - Root cause analysis

CITY OF Saco
www.SacoMaine.org

Additional email licensing

- Request: Boards, committees, and non-computer user staff do not have a @sacomaine.org email address. An issue we have identified is the inability to search and produce FOAA requested information on discussions that occur between these boards and committees that use personal email accounts.
- Expense: 11,020/year ~ 155 licenses

CITY OF Saco
www.SacoMaine.org