Annual Report - 2022

Information Technology Department | St. Joseph County, Michigan Government

It was a year of audits and assessments for the St. Joseph County Information Technology Department in 2022. Multiple third-party assessments of many different county departments validated St. Joseph County's progress towards the implementation of cyber security best practices and established frameworks.

Industry trends and requirements from Federal partners, insurers, and government related industries continue to push local government to implement the latest in security technologies. New projects, such as the implementation of internal and external vulnerability scanning platforms, new vulnerability management procedures, as well as improved email protections show St. Joseph county's commitment to continuous improvement in our cyber security posture.

As technology continues to make local government more efficient and allow municipalities to offer new services to their citizens, the St. Joseph County IT Department continues to focus on improving the protection of sensitive information and the security of county systems that are vital to the performance of critical government services.

Sincerely,

Dustin Bainbridge, CISM, CGCIO
Director of Information Technology

The Role of Information Technology

Information Technology by the Numbers:
Supported Computers: 325+
VoIP Telephones: 140+
Printers and FAX Machines: 90+
Servers: 50+
Network Infrastructure and Security Devices: 60+
Computer Users: 350+
Production Data Size: 40+ Terabytes
Annual Help Desk/Email/Telephone Requests: 2,200+
Annual Computer Replacements/Upgrades: ≈ 60

The primary mission of the Information Technology Department is to provide quality infrastructure, support, and innovation in the planning, development, and deployment of state-of-the-art information and communication technology systems and services to enable and empower the departments, offices, and officials of the St. Joseph County Government.

The IT Department implements, maintains, and supports the data and telecommunications hardware and software to all the county departments and offices. Additionally, the county IT Department supports all St. Joseph County law enforcement agencies and fire and rescue services in their access to county provided public safety computer systems and in-vehicle computers. The IT Department supports over 1000 devices and over 50 separate software systems used by county departments to provide public services in addition to many utility, compliance, and security computer systems. Supported technologies include but are not limited to:

- Computers, Printers, Scanners
- Document Imaging Systems
- Case/Records Management
- Email
- Telephones, FAX and Voice Systems
- Property Records Systems
- Videoconferencing
- Courtroom Proceedings Video
- Law Enforcement Vehicle Video
- Security Cameras and Video, Doors Locks and Access Cards
- Collaboration and Messaging Software
- Remote Access Systems
- Financial Management Systems
- Cloud Storage and Sharing Services
- Cyber Security Systems and Software
- Data Center and Server Equipment
- Network Equipment and Infrastructure

Personnel

The IT Department consists of the Director, System Administrator, Network Analyst, Technician, and a document imaging support contractor. The Network Analyst position is funded by the St. Joseph County 911 Central Dispatch under the agreement that the IT Department will provide the equivalent of one position in support of 911 Central Dispatch and select support of external law enforcement agencies and fire and rescue services. The equivalent of three positions is available to support of all other county departments including the general departments, county courts, and the Commission on Aging in addition to performing all necessary server and system maintenance, cybersecurity and data governance tasks, and vendor data security validations. IT staff are on-call 24/7/365 in support of 24-hour departments and are frequently called upon outside of normal business hours for support and maintenance tasks.

With the adoption of remote work in the technology sector, the IT Department is competing at a nation-wide level for acquisition and retention of talent. Investment in our staff will continue to be vital for staff retention and to provide consistency within the department and continued legacy knowledge for the organization.

Financials – 2022

General Fund (Excluding Personnel Accounts)	Budgeted	Activity
Office Supplies (Ink, Toner, Keyboard, Mouse, Small Technology Products)	10,000	7,242
Other Supplies (Network cable, Tools)	2,000	2,033
Dues & Memberships	200	0
Contractual Services	64,000	47,207
Internet and Website Hosting	30,000	18,739
Travel	700	191
Training & Profession Development (IT Staff Training, OnBase Training, Employee Cyber Security Awareness)	16,600	9,167
Computer Maintenance and Service Contracts (Software Maintenance, Office 365 Subscription, Hardware Maintenance, etc.)	318,119	330,923
Computer Maintenance and Service Contracts – MDT (Electronic Citation Software Maintenance)	15,000	0
Telephone Maintenance and Service Contracts (Telephone System Licensing and Maintenance)	27,780	30,293
Computer Hardware (Servers, Network Equipment)	8,000	24,889
Computer Hardware - MDT	0	1,208
Computer Software	3,000	0
Telephone Equipment	1,000	374
Total General Fund Expenses (Including personnel and other accounts)	773,108	770,499
Capital Fund (Servers, network equipment, telephone equipment, etc.)	77,052	79,476

Notes: The expenses above do not show the full amount of St. Joseph County's technology investments as some expenses are not allocated to the IT Department's budget and are not funded from the General Fund.

The technology industry's movement towards "as a service" billing and cloud computing has and will continue to move large capital investments in technology into annual operational and maintenance expenses.

Technology Highlights - 2022

Criminal Justice Information System Security Audits
The FBI maintains the Criminal Justice Information System Security Policy (CJISSECPOL) which details rules and requirements that must be in place and followed by any departments that access, process, and store data derived from the NCIC and LEIN. These requirements are largely derived from a cybersecurity framework established by the National Institute for Standards and Technology (NIST).

Affected St. Joseph County departments include District and Circuit Courts, Prosecutor's Office, Sheriff's Department and e911 Central Dispatch.

The Michigan State Police perform an individual audit of each department on their adherence to the CJISSECPOL, typically every three years. Failure to adhere to the CJISSECPOL could result in loss of local control of criminal justice computer systems and loss of access to criminal justice information which would severely hinder the ability for local law enforcement and county departments to provide vital services.

Due to the technical nature of many requirements, the IT Department is significantly involved in these audits and works closely with affected departments to achieve CJISSECPOL compliance. The stages of each audit's lifecycle, including preparation, responding to pre-audit questionnaires, Q & A sessions with auditors, and non-compliance response and remediation, typically involve assistance, materials, and input from the IT Department.

In 2022, the above-mentioned St. Joseph County departments received good reports in their audits with few technology-related non-compliance findings. Further updates to the CJISSECPOL for 2023 and 2024 necessitate additional cyber security policies, controls, and systems for the county to continue be compliant for expected audits in early 2025. Additional technology controls are planned for implementation by the end of 2024.

Email Security Improvements
Email remains the number one threat vector for cyberattacks whether it be ransomware, fraud, spoofing attacks, or phishing scams that attempt to steal employee credentials. To further protect from email threats, we implemented an additional email security product that helps to better identify email threats and to inform county staff of external emails and spoofing attacks.

IRS Publication 1075 Audit and CIS Security Controls
The IRS maintains IRS Publication 1075, which is similar in concept to the CJISSECPOL but regarding Federal Tax Information. While also based on standards set by NIST, IRS Pub 1075 has its own rules and requirements.

The State of Michigan's Department of Health and Human Services (DHHS) audits the adherence of St. Joseph County's Friend of the Court office to IRS Pub 1075, typically every three years. In 2022, DHHS elected to perform this audit as an assessment of St. Joseph County's implementation to the Center for Internet Security's (CIS) Critical Security Controls and with a one-time vulnerability scan of St. Joseph County's network.

The CIS Critical Security Controls is a separate cyber security framework that allows for easier scoring of an organization's cyber security posture and deliverables to show progress, improvements, and security maturity.

Overall St. Joseph County scored well on the audit but there is room for improvement in our adoption of the CIS Critical Security Controls as a cybersecurity framework. Non-compliance findings and detected vulnerabilities as well as plans for their remediation were outlined in a Plan of Action and Milestones (POAM) by the IT Director. The IT Department continues to have monthly meetings with the assessment providers on the progress of the St. Joseph County Government's implementation of the CIS Controls and the audit POAM. Discovered vulnerabilities were quickly mitigated. Further implementation of the CIS Controls will result in several new county policies that will be presented to the Board of Commissioners for approval in the coming months.

Vulnerability Scanning and Management
The implementation of a vulnerability scanner and management system in 2022 has significantly improved the time it takes for vulnerabilities to be identified and resolved through the organization. Third party patching systems have allowed for software updates to be primarily automated which has allowed the IT Department to meet industry best practices with vulnerability management and meet vulnerability management and patching controls outlined in the CIS Critical Security Controls.