TIOGA COUNTY, NEW YORK
Information Technology and Communication Services
Ronald E. Dougherty County Office Building 56 Main Street Owego, NY 13827
**Jeremy Loveland** Chief Information Officer 607 687 8294 607 223 7004 www.TiogaCountyNY.gov

# Information Technology – Legislative Committee Meeting

## 12.03.24

- APPROVAL OF MINUTES
    - 11.05.24 IT Legislative Committee Meeting
- FINANCIAL
    - Review of Budget Status and Financial News
- OLD BUSINESS
    - Waverly MH Update
    - IT Climate Survey Update
- NEW BUSINESS
    - CIO Entry Plan (Strategic Plan) Report
    - New York State Digital Orthoimagery Program (NYSDOP)
- PERSONNEL
    - Nothing to Report
- RESOLUTIONS
    - L19 - AUTHORIZE AGREEMENT WITH SOUTHERN TIER NETWORKS FOR DARK FIBER STRANDS
    - L48 - AMEND EMPLOYEE HANDBOOK; SECTION VIII: COMPREHENSIVE INFORMATION SECURITY POLICY
- PROCLAMATIONS
    - Nothing to Report
- ADJOURNMENT

TIOGA COUNTY, NEW YORK
Information Technology and Communication Services
Ronald E. Dougherty County Office Building 56 Main Street Owego, NY 13827
Jeremy Loveland Chief Information Officer 607 687 8294 607 223 7004 www.TiogaCountyNY.gov

INFORMATION TECHNOLOGY LEGISLATIVE STANDING COMMITTEE

November 5th, 2024, at 9:30 am

ATTENDANCE:

- Legislators: Jake Brown, Tracy Monell, Dennis Mullen, Ron Ciotoli, William Standinger, Martha Sauerbey.
- Staff: Jeremy Loveland, CIO; Brandon Clark, Deputy Director of ITCS
- Guests: Cathy Haskell, Peter DeWind, Jackson Bailey

- APPROVAL OF MINUTES: Approval of October 8th, 2024, Information Technology Committee Minutes: Legislator Tracy Monell made the motion, seconded by Legislator Dennis Mullen to approve the October 8th, 2024, Information Technology Committee Minutes as written. Motion carried.

- FINANCIAL
  - Review of budget status and financial news

- OLD BUSINESS
  - VESTA Fiber Circuit
    - An in-depth discussion took place regarding the status of the alternate 911 center and the priority of implementing the existing fiber circuit between the Tioga County Public Safety building and alternate 911 center location.
  - CAC Relocation Update
    - The ITCS Department has completed the technical requirements of the CAC office relocation project.

- NEW BUSINESS
  - IT Climate Survey
    - The ITCS Department will be releasing its 3-year IT climate survey to the users within Tioga County and the Shared Service agencies this month.

DRAFT

- Strategic Plan Update Schedule
    - The schedule was discussed for reporting on the existing IT strategic plan and reviewing the strategic plan for 2025 – 2028.
- PERSONNEL
    - Nothing to Report
- RESOLUTIONS/PROCLAMATIONS
    - K13 – AUTHORIZE AGREEMENT ADDENDUM WITH NEW YORK STATE INFORMATION TECHNOLOGY SERVICES FOR ENDPOINT DETECTION AND RESPONSE SOFTWARE.
- ADJOURNMENT
    - Legislator Monell motioned to adjourn at 9:55 a.m., seconded by Legislator Brown.

DRAFT

# Review of 2024 Budget and Financial News

## A1680 – Year-to-Date Budget Report

FOR 2024 12

| ACCOUNTS FOR: A General Fund | | ORIGINAL APPROP | TRANFRS/ ADJSTMTS | REVISED BUDGET | YTD ACTUAL | ENCUMBRANCES | AVAILABLE BUDGET | PCT USE/COL |
|---|---|---|---|---|---|---|---|---|
| A1680 Information Technology | | | | | | | | |
| A1680 412702 | Shared Services- I | -210,072 | 0 | -210,072 | -212,490.06 | .00 | 2,418.06 | 101.2% |
| A1680 412707 | Shared Services- E | -90,000 | 0 | -90,000 | -.07 | .00 | -89,999.93 | .0%* |
| A1680 422280 | Data Processing/Pr | 0 | 0 | 0 | -2,181.23 | .00 | 2,181.23 | 100.0% |
| A1680 424100 | Rental Of County O | -5,000 | 0 | -5,000 | -6,550.08 | .00 | 1,550.08 | 131.0% |
| A1680 427010 | Refunds Of Prior Y | 0 | 0 | 0 | -1,590.00 | .00 | 1,590.00 | 100.0% |
| A1680 510010 | Full Time | 562,076 | 0 | 562,076 | 459,502.17 | .00 | 102,573.83 | 81.8% |
| A1680 540070 | Car Maintenance | 500 | 0 | 500 | 362.99 | .00 | 137.01 | 72.6% |
| A1680 540140 | Contracting Servic | 28,880 | -200 | 28,680 | 17,429.09 | .00 | 11,250.91 | 60.8% |
| A1680 540140 | M7674 Contracting S | 0 | 141,723 | 141,723 | 96,005.44 | .00 | 45,717.48 | 67.7% |
| A1680 540180 | Dues | 50 | 0 | 50 | 50.00 | .00 | .00 | 100.0% |
| A1680 540220 | Automobile Fuel | 800 | 0 | 800 | 528.36 | .00 | 271.64 | 66.0% |
| A1680 540320 | Leased/Service Equ | 5,500 | 5,000 | 10,500 | -363.73 | .00 | 10,863.73 | -3.5% |
| A1680 540350 | Office Equip Maint | 25,000 | -5,000 | 20,000 | 19,553.08 | .00 | 446.92 | 97.8% |
| A1680 540420 | Office Supplies | 1,500 | 0 | 1,500 | 345.58 | .00 | 1,154.42 | 23.0% |
| A1680 540480 | Postage | 0 | 200 | 200 | 1.28 | .00 | 198.72 | .6% |
| A1680 540485 | Printing/Paper | 1,000 | 0 | 1,000 | .00 | .00 | 1,000.00 | .0% |
| A1680 540620 | Software Expense | 207,340 | 0 | 207,340 | 72,985.81 | 120,992.40 | 13,362.28 | 93.6% |
| A1680 540640 | Supplies (Not Offi | 4,500 | 0 | 4,500 | 3,791.32 | .00 | 708.68 | 84.3% |
| A1680 540640 | SSG21 Supplies (Not | 2,500 | 0 | 2,500 | .00 | .00 | 2,500.00 | .0% |
| A1680 540660 | Telephone | 72,500 | 0 | 72,500 | 44,447.61 | 134.00 | 27,918.39 | 61.5% |
| A1680 540661 | Telephone Maintena | 24,500 | 0 | 24,500 | 22,923.69 | .00 | 1,576.31 | 93.6% |
| A1680 540733 | Training/All Other | 5,000 | 0 | 5,000 | 2,705.29 | .00 | 2,294.71 | 54.1% |
| A1680 581088 | State Retirement F | 15,932 | 41,210 | 57,142 | 51,202.13 | .00 | 5,939.64 | 89.6% |
| A1680 583088 | Social Security Fr | 39,959 | -6,962 | 32,997 | 35,222.91 | .00 | -2,225.80 | 106.7%* |
| A1680 584088 | Workers Compensati | 0 | 8,673 | 8,673 | 8,686.44 | .00 | -12.96 | 100.1%* |
| A1680 585588 | Disability Insuran | 0 | 460 | 460 | 493.29 | .00 | -33.63 | 107.3%* |
| A1680 586088 | Health Insurance F | 22,536 | 105,536 | 128,072 | 119,467.14 | .00 | 8,604.80 | 93.3% |
| A1680 588988 | Eap Fringe | 0 | 114 | 114 | 115.29 | .00 | -1.23 | 101.1%* |
| TOTAL Information Technology | | 715,001 | 290,754 | 1,005,755 | 732,643.74 | 121,126.40 | 151,985.29 | 84.9% |
| TOTAL General Fund | | 715,001 | 290,754 | 1,005,755 | 732,643.74 | 121,126.40 | 151,985.29 | 84.9% |
| | TOTAL REVENUES | -305,072 | 0 | -305,072 | -222,811.44 | .00 | -82,260.56 | |
| | TOTAL EXPENSES | 1,020,073 | 290,754 | 1,310,827 | 955,455.18 | 121,126.40 | 234,245.85 | |

FOR 2024 12

| | ORIGINAL APPROP | TRANFRS/ ADJSTMTS | REVISED BUDGET | YTD ACTUAL | ENCUMBRANCES | AVAILABLE BUDGET | PCT USE/COL |
|---|---|---|---|---|---|---|---|
| GRAND TOTAL | 715,001 | 290,754 | 1,005,755 | 732,643.74 | 121,126.40 | 151,985.29 | 84.9% |

# H1680 – Year-to-Date Capital Budget Report

FOR 2024 12

| ACCOUNTS FOR: H Capital Fund | ORIGINAL APPROP | TRANFRS/ ADJSTMTS | REVISED BUDGET | YTD ACTUAL | ENCUMBRANCES | AVAILABLE BUDGET | PCT USE/COL |
|---|---|---|---|---|---|---|---|
| H1680 Information Technology | | | | | | | |
| H1680 520620 Software Expense | 142,313 | 175,309 | 317,621 | 296,435.37 | 20,673.50 | 512.26 | 99.8% |
| H1680 520620 M7674 Software Expe | 0 | 39,251 | 39,251 | .00 | .00 | 39,250.67 | .0% |
| H1680 521090 Computer | 102,000 | 0 | 102,000 | 64,715.97 | 1,164.00 | 36,120.03 | 64.6% |
| TOTAL Information Technology | 244,313 | 214,559 | 458,872 | 361,151.34 | 21,837.50 | 75,882.96 | 83.5% |
| TOTAL Capital Fund | 244,313 | 214,559 | 458,872 | 361,151.34 | 21,837.50 | 75,882.96 | 83.5% |
| TOTAL EXPENSES | 244,313 | 214,559 | 458,872 | 361,151.34 | 21,837.50 | 75,882.96 | |

FOR 2024 12

| | ORIGINAL APPROP | TRANFRS/ ADJSTMTS | REVISED BUDGET | YTD ACTUAL | ENCUMBRANCES | AVAILABLE BUDGET | PCT USE/COL |
|---|---|---|---|---|---|---|---|
| GRAND TOTAL | 244,313 | 214,559 | 458,872 | 361,151.34 | 21,837.50 | 75,882.96 | 83.5% |

# LEADERSHIP

**"Effective leadership fosters a mission-focused, team-centric environment while focusing on the development of other leaders through communication, accountability and empowerment."**

## ENTRY FEEDBACK AND INPUT

- Need for decisive leadership within the ITCS Department
- Professional development of ITCS staff
- Legislature placed an emphasis on deck plate leadership within the department
- Increase collaboration of the IT Steering Committee
- Limited information and communication coming from the ITCS Department
- Equal distribution of resources (hardware and human) across all departments and buildings
- Upgrade and update the County website; simplify maintenance of website
- Increase collaboration within County

## DEFINED GOALS

1. Increase both department and inter-departmental communication and workflow processes to increase efficiency throughout the County
2. Develop and foster a team-centered, collaborative and professional work environment
3. Develop and increase IT skillsets within the ITCS department.
4. Investigate and deploy strategies for maintaining fiscal responsibility while maintaining and growing essential IT services and support throughout Tioga County

*"The key to success in any organization is identifying, developing, and empowering the right people."*

- Craig Groeschel

*"The difference between mere management and leadership is communication."*

- Winston Churchill

| Defined Goal Number One:<br><br>Increase both departmental and interdepartmental communication and workflow processes to increase efficiency throughout the County. | |
|---|---|
| Action Item | Implement Microsoft Office 365 throughout the County to provide automated workflow processes, shared calendars, and collaborative tools required to foster an atmosphere with increased teamwork throughout the County. |
| Status | Microsoft Office 365 has been implemented through the County. All Tioga County users have been migrated using G3 licenses. All Tioga County users have been migrated from on-premises Microsoft Exchange to Exchange Online.<br><br>Some outstanding items for this item are to fully implement Microsoft OneDrive and migrated user files from the County File Server. We would also like to work with the Shared Service agencies to investigate the feasibility of migrating their users to Office 365 and decommission the on-premises Microsoft Exchange server. |
| Action Item | Develop an online County ITCS service status board, offering live data on the status of the various IT services provided by the ITCS Department |
| Status | The ITCS Department has invested in an IT Service Management (ITSM) platform called FreshService. Among several ITSM tools, Freshservice provides the ability to develop a status board reflecting the current status of all systems and service provided or maintained by the ITCS Department. This also allows the ITCS Department to communicate upcoming maintenance windows and allows our users to subscribe to specific services or systems they would like to be notified about. This allows targeted communication and minimizes the risk of over-communicating about issues the users may not be concerned with.<br><br>This status board is planned for implementation in quarter one of 2025. |
| Action Item | Evaluate current trouble ticket processes, identify additional functionality needs, and develop a trouble ticket strategy to increase communication between the ITCS Department and the end-users regarding the status of and work being completed on their submitted trouble tickets. |
| Status | A deep analysis was completed, and it was determined that a robust IT Service Management platform is needed for use throughout the Tioga County infrastructure. Multiple ITSM platforms were researched and demonstrated, with the final product selection being FreshService.<br><br>The new 'Tioga County Service Center (TCSC)' is being implemented in quarter four of 2024. The vision for the TCSC is to be a single platform for all employees to request service or assistance, regardless of department. For instance, if a user has a buildings and grounds request, they can request it here as well. If a user has a cleaning request, they can also request it here.<br><br>ITCS staff have been introduced to the platform and will continue their professional development through the onboarding process provided by FreshService. |
| Action Item | Develop and implement robust Change Management (CM) tracking and end-user notification process. |
| Status | In addition to the ticket management system provided by the new Tioga County Service Center (TCSC), it includes a Change Management (CM) platform. The CM platform will be used by ITCS staff to request, approve, track, and document all IT changes throughout the Tioga County infrastructure.<br><br>A Change Advisory Board (CAB) has been identified and will begin meeting weekly to complete the vetting process for all IT changes, starting in January 2025.<br><br>All upcoming changes will be communicated using the IT Service Status Board, also located in the Tioga County Service Center (TCSC). |
| Action Item | Develop a County Website Committee to review the current County website, identify existing short-comings and future needs. If required, this committee will be the catalyst for change for the optics and functionality provided to our public via the County website. |

| | |
|---|---|
| Status | While initial research and product demonstrations have been done to address this action item, it will need to be carried over into the next strategic plan. |
| Action Item | Investigate feasibility of using Chromebooks and Chromeboxes throughout Tioga County for general use, digital signage and Legislator use. |
| Status | ITCS staff has worked with Google to attempt the establishment of a Google Workspace for the County. Unfortunately, this has not been completed and has proven difficult and not mutually beneficial to continue to pursue. |
| Defined Goal Number Two:<br><br>Develop and foster a team-centered, collaborative and professional work environment | |
| Action Item | Continue bi-weekly ITCS Department meetings to discuss projects and provide opportunities for team members to participate fully in all current departmental projects. |
| Status | This process has continued through the duration of the last three years. Increased buy-in, understanding, and communication has been experienced. ITCS Department leadership has witnessed a positive culture shift, simply by including all team members in all projects within the Department. |
| Action Item | Educate, equip, and empower ITCS team members to manage their workload and make decisions. I firmly believe an accurate indicator of how empowered team members are is determining how low in the organization someone has the authority to say, "yes." |
| Status | This will continue to be a point of emphasis for the leadership team within the ITCS Department. It has taken time to implement this leadership philosophy, but I'm happy to report that it is catching on. Our team members understand their expectations and their ability to make decisions within those expectations without having to ask permission.<br><br>We are also continuing to focus, as supervisors, to be ok with the decisions and outcome of those decisions, regardless of how they may or may not align with the quality of work that we would have personally done. The main concern is that the mission is accomplished, not that it gets accomplished how we would accomplish it all the time.<br><br>This is another action item that will continue in the next strategic plan as it should always be a point of emphasis. |
| Defined Goal Number Three:<br><br>Develop and Increase Information Technology skillsets within the ITCS Department | |
| Action Item | Develop departmental, cross-training Professional Development strategies designed toward both maintaining and developing additional IT skillsets within the ITCS Department. |
| Status | Professional Development has been implemented in a variety of ways within the ITCS Department. Mainly, it is accomplished using a subscription to Udemy Business. The expectation for all staff within the Department is to spend a minimum of 2 hours per week on some sort of professional development using this platform.<br><br>Additional training, particularly cross-training, is completed throughout the various staff meetings throughout the year. |
| Action Item | Identify and pursue Professional Development seminars, conferences or workshops throughout the region. |
| Status | Professional Development opportunities within our region and within our budget have proven to be difficult to find. While this action item continues to be at the forefront of our professional development goal, until opportunities present themselves, this will continue to be unmet. |

| | |
|---|---|
| Action Item | Continue partnership with NYSGLITDA to foster an atmosphere of information and knowledge sharing between New York State Governmental Information Technology entities. |
| Status | The ITCS Department maintains its membership with NYSLITDA and has attended one of their bi-annual conferences each year. |
| Defined Goal Number Four:<br><br>Investigate and deploy strategies for maintaining fiscal responsibility while maintaining and growing essential IT services and support throughout Tioga County | |
| Action Item | Execute plan to bring the Village of Owego and the Town of Candor as Tioga County IT Shared Services entities. |
| Status | Both the Village of Owego and the Town of Candor have successfully been added as IT Shared Service entities for Tioga County. |
| Action Item | Investigate and implement additional strategies and opportunities to grow IT Shared Services throughout Tioga County. |
| Status | As broadband and high-speed networks continue to be built throughout the County, there have been opportunities to expand IT Shared Services throughout the County. One of municipalities added to the County's IT Shared Service program is the Town of Nichols. |
| Action Item | Develop and maintain a robust five (5) year strategic IT planning document highlighting budgeting priorities and planned capital projects. |
| Status | A robust capital project plan has been established and maintained over the last several years. All capital project planning is now proactive, meaning the County is breaking the cost of those projects up and budgeting per year for those cost, placing money in reserve accounts earmarked for those projects. This allows for a more consistent capital budget from year to year. |

# SUPPORT

**"Building a good customer experience does not happen by accident. It happens by design."**

Anonymous

## ENTRY FEEDBACK AND INPUT

- Climate survey results were encouraging.
- Interviews with staff, Department Heads and Legislators were all very positive.
- Remote Support services need improved and standardized
- Current ticket management system lacks reporting capabilities. Email submission is the only form of submission
- Tier 2 level IT skillset needs improved / increased
- Currently no IT Professional Development being offered outside of the GIS application Professional Development
- A major finding in the climate survey was improving printing and copying services

## DEFINED GOALS

1. Prioritize Professional Development
2. Improve Printing and Copying Services
3. Pursue and implement proven support best-practices within ITCS Department
4. Maintain and improve IT Infrastructure throughout the County

*"When I think about great service, it's about how you take every interaction you have with the customer and use that as a way to improve their perception of your organization."*

- John Herstein

*"Quality in a service or product is not what you put into it. It is what the client or customer gets out of it."*

- Peter F. Drucker

| Defined Goal Number One:<br><br>Prioritize Professional Development | |
|---|---|
| Action Item | Develop departmental, cross-training Professional Development strategies designed toward both maintaining and developing additional IT skillsets within the ITCS Department. |
| Status | Professional Development has been implemented in a variety of ways within the ITCS Department. Mainly, it is accomplished using a subscription to Udemy Business. The expectation for all staff within the Department is to spend a minimum of 2 hours per week on some sort of professional development using this platform.<br><br>Additional training, particularly cross-training, is completed throughout the various staff meetings throughout the year. |
| Action Item | Develop and implement a robust and continuous Information Technology Professional Development strategy for all Tioga County and Shared Service employees. |
| Status | Annual IT Professional Development opportunities have been provided to all users, including Shared Service employees. Topics such as Office 365 applications, Web site maintenance, Outlook, and OneDrive have all been provided.<br><br>While participation remains low, the ITCS Department aims to maintain training opportunities for its users. |
| Defined Goal Number Two:<br><br>Improve printing and copying services | |
| Action Item | Complete a detailed analysis of existing lease agreements on copiers. Seek competitor pricing and model comparisons. Evaluate current copy leases to determine whether to continue partnership at the end of the lease agreements. |
| Status | A complete and detailed analysis of existing lease agreements was completed. Vendor comparisons were completed. While many of the lease agreements utilized very aggressive pricing, the support for those devices remained quite low.<br><br>After addressing those concerns with the current vendor, it was decided to maintain most of its copier fleet with the current vendor. The main contributing factor was pricing. |
| Action Item | Complete a detailed analysis of all non-copy printing devices in order to ensure right-sizing and proper printing locations. |
| Status | Analysis has been completed regarding the non-copy printing devices on the County network. There have not been any changes implemented based on the findings of this analysis currently. |
| Action Item | Investigate and implement a Managed Print Services (MPS) agreement for all non-copier printing devices. An MPS will standardize and simplify the management, repair, and toner logistics for all County devices. |
| Status | A detailed investigation for available MPS programs from two different vendors was completed. Neither of the program quotes provided significant savings expected from a Managed Print Services agreement. This action item should continue over the next strategic plan as it would provide significant value to the County, if the proper program can be aligned to our printing needs. |

| Defined Goal Number Three:<br><br>Pursue and implement proven support best-practices within ITCS Department | |
|---|---|
| Action Item | Investigate, develop and implement a Ticket Management System (TMS) which improves ITCS department to use communication. The TMS should also allow data to be analyzed periodically to provide statistical data used for decision-making and determining Professional Development priorities. |
| Status | A deep analysis was completed, and it was determined that a robust IT Service Management platform is needed for use throughout the Tioga County infrastructure. Multiple ITSM platforms were researched and demonstrated, with the final product selection being FreshService.<br><br>The new 'Tioga County Service Center (TCSC)' is being implemented in quarter four of 2024. The vision for the TCSC is to be a single platform for all employees to request service or assistance, regardless of department. For instance, if a user has a buildings and grounds request, they can request it here as well. If a user has a cleaning request, they can also request it here.<br><br>ITCS staff have been introduced to the platform and will continue their professional development through the onboarding process provided by FreshService. |
| Action Item | Document and diagram all Tioga County IT networks and systems. Maintain an annual review process designed to ensure the validity of this documentation. |
| Status | Several portions of the Tioga County network have been property investigated and documented.<br><br>Additional staff members have been added with the skillsets required to continue with this action item. This, along with the implementation of proper Change Management (CM) and alignment with NIST 800-53 standards, will provide a framework to follow as this action item progresses. |
| Action Item | Develop an online County ITCS service status board, offering live data on the status of the various IT services provided by the ITCS department. |
| Status | As a part of the implementation of the ITSM tool, Freshservice, an IT status board is included. This status board provides a current snapshot of the status of all IT services. This is also how the ITCS department communicates outages and planned maintenance windows with its users. |
| Action Item | Investigate, develop and implement network monitoring services for all Tioga County IT networks and systems providing 24/7 monitoring and notification services. |
| Status | While a true network monitoring platform has not been implemented, several tools, including a Remote Monitoring and Management (RMM) tool called NinjaOne has been implemented. This allows ITCS staff members to be notified if services, systems, or network go offline.<br><br>In addition to NinjaOne, several network devices have been migrated to the UniFi platform, which inherently provides a self-monitoring system which will notify ITCS staff of outages.<br><br>A robust network monitoring system should continue to be an action item. |
| Action Item | Develop and implement Standard Operating Procedure (SOP) program to ensure all essential tasks are documented and reviewed annually to ensure validity of information within the documents. |
| Status | Also included in the ITSM took, FreshService, is a function called Solutions. This platform allows ITCS Staff to document standard operating procedures and track their review dates automatically.<br><br>While this has not been implemented yet, it is planned for FY2025. |

| Defined Goal Number Four:<br><br>Maintain and Improve IT Infrastructure throughout the County | |
|---|---|
| Action Item | Migrate current on-premises Microsoft Exchange 2019 server to Microsoft Exchange Online. This reduces cost of maintenance, while improving the collaboration of services between other Microsoft Office 365 applications and services. |
| Status | Microsoft Exchange Online has been implemented to our Exchange Environment. There are several factors leading to the continued use and maintenance of the on-premises Exchange 2019 server. Mainly, the dependence of our IT Shared Service agencies who are not participating in Office 365 subscriptions. In order to fully decommission the Exchange 2019 server all users would need to subscribe annually to Microsoft's Office 365 program. This would significantly increase the cost of services provided to the municipality and is not feasible at this time.<br><br>All Tioga County users have been migrated from the on-premises server to Exchange Online. |
| Action Item | Replace End-of-Life (EOL) Server Hosts with supported hardware. Current hardware is no longer supported by VMWare nor HPe. |
| Status | All server host hardware has been replaced with updated and supported server hardware. This new hardware is supported via reseller warranty, VMWare and HPe. |
| Action Item | Complete analysis and review of current Wireless Network Infrastructure. Current system is a Cisco system, with many Wireless Access Points (WAPs) being purchased used, from eBay. |
| Status | The wireless network infrastructure throughout the County and all Shared Service entities has been replaced using new UniFi Access Points. |
| Action Item | Upgrade Storage Area Network (SAN) arrays with devices supporting increased data compression and Data-at-Rest (DAR) encryption. |
| Status | All Storage Area Network (SAN) arrays were upgraded to devices supporting increased data compression and data-at-Rest (DAR) encryption. All SAN devices are covered by manufacturer warranty and are supported by the reseller. |
| Action | Upgrade Sophos Firewall devices with current hardware supporting SSL decryption. |
| Status | All Sophos firewalls were replaced with upgraded models which support SSL decryption. Those devices are also supported by the reseller and manufacturer warranty. Additional firewall resources have allowed for additional configuration and functionality providing additional security services to the County and its IT Shared Service entities. |

# SECURITY

**"One single vulnerability is all an attacker needs."**

Window Snyder

## ENTRY FEEDBACK AND INPUT

- Independent Cyber Security Audit found the following major findings: Data-at-Rest (DAR) Encryption, Multi-Factor Authentication, Access Control monitoring
- Lack of Change Management Process
- Sufficient processes for keeping software patched and updated
- Lack of hardware / software discovery reporting
- Insufficient restrictions on removeable storage devices
- Complete annual Phishing campaigns to raise awareness with users
- Lack of consistent physical access control and security camera systems
- Information Security Officer Job Description needs reviewed

## DEFINED GOALS

1. Establish Cyber and Infrastructure Security as a main pillar of Tioga County ITCS services and support.

2. Pursue security best practice implementation at Tioga County.

3. Introduce and maintain transparency and accountability throughout all Tioga County ITCS services and support.

*"There are only two types of companies: those that have been hacked, and those that will be hacked. Even that is merging into one category: those that have been hacked and will be again."*

- Robert Mueller

*"Security is not a product, but a process."*

- Bruce Schneier

SEAL OF TIOGA COUNTY, NEW YORK

| Defined Goal Number One:<br><br>Establish cyber and infrastructure security as a main pillar of Tioga County ITCS services and support | |
|---|---|
| Action Item | Continue assisting the Information Security Officer (ISO) with the development and implementation of a Business Continuity Management (BCM) policy and plan. |
| Status | The Business Management and Continuity Plan was completed by the third-party vendor hired for this project. |
| Action Item | Partner with the Information Security Officer (ISO) in the development and implementation of targeted information campaigns regarding Information Security topics for all Tioga County users. |
| Status | Multiple strategies have been employed to cover various training areas within the area of Information and Cyber Security. While targeted training campaigns were attempted, it was proven to be ineffective. Rather than using several smaller campaigns, it was determined that a more robust annual Cyber Security training requirement would best satisfy this action item. As such, the annual Cyber Security training material and retention requirement was bolstered. |
| Action Item | Actively participate in annual table-top cyber security exercises planned and executed by the Information Security Officer. |
| Status | This action item has not been completed. There are several reasons for it, including the shift from the current ISO being in the Legislative Office and being brought into the ITCS Department. This shift meant hiring a new Deputy Director with skills and experience capable of satisfying the ISO responsibilities.<br><br>This action item will be included in the next strategic plan as well. |
| Action Item | Review Information Security Officer (ISO) job description to ensure all essential roles and responsibilities are included. |
| Status | The Information Security Officer (ISO) job description was reviewed, and all essential roles and responsibilities were added to the Deputy Director of Information Technology and Communication Services Department job description. |
| Action Item | Complete bi-annual anti-phishing campaigns for all Tioga County users to ensure users are trained and are practicing safeguards against Phishing attacks. |
| Status | Anti-phishing campaigns are randomly generated and sent to portions of Tioga County and Shared Service entity users throughout the year. This provides more robust coverage of our users as they don't know when or if they'll receive phishing types of emails. |
| Defined Goal Number Two:<br><br>Pursue security best practice implementation at Tioga County | |
| Action Item | Upgrade existing Storage Area Network (SAN) devices with hardware the supports Data-at-Rest (DAR) encryption and provide an improved disaster recovery feature-set. |
| Status | All Storage Area Network (SAN) arrays were upgraded to devices supporting increased data compression and data-at-Rest (DAR) encryption. All SAN devices are covered by manufacturer warranty and are supported by the reseller. |
| Action Item | Develop and implement a robust data backup / Disaster Recovery (DR) strategy. |
| | |

| | |
|---|---|
| Status | The current Disaster Recovery strategy, which comprised of data and site replication more than a data backup strategy, was completely overhauled. An onsite Disaster Recovery appliance was implemented. An additional off-site, off-line Disaster Recovery appliance was also implemented to provide additional protection from ransomware attacks. |
| Action Item | Implement Multi-Factor Authentication (MFA) to access Tioga County resources externally. |
| Status | Multi-Factor Authentication (MFA) has been implemented County and Shared Service entity-wide for accessing internal County resources from external resources. The County uses integrated MFA functionality of existing systems to meet this requirement. |
| Action Item | Subscribe to and implement Access Control management and reporting software for all Tioga County networks and systems. |
| Status | In addition to the monitoring functionality of NinjaOne, it also provides a secure remote access management platform for users to access internal resources (computers). This has been implemented to replace the existing remote access system using a web-enabled SSL VPN portal. |
| Action Item | Complete the migration of all Board of Elections devices to a separate and protected network segment. |
| Status | **Withheld due to Cybersecurity concerns** |
| Action Item | Comply with and enforce established password management procedures defined in the Comprehensive Information Security Policy. |
| Status | The Comprehensive Information Security Policy has been updated to align with NIST 800-53 requirements, including the establishment and use of passwords within the County and Shared Service entities. |
| Action Item | Investigate, develop and implement a consistent, standard building access control system within Tioga County. |
| Status | A consistent, standard building access control system has been implemented throughout all buildings (except Public Safety) with existing access control systems. Additional access control systems have been installed in other areas within the County and Shared Service entities. Each of these systems use the same ecosystem and provide a centrally managed platform for each building. |
| Action Item | Remove all generic network and system accounts with elevated privileges. All elevated accounts need to be associated with a specific user. |
| Status | All generic network and system accounts with elevated privileges have been deleted. All elevated accounts are associated with specific users. |
| Action Item | Investigate, develop and implement a consistent, standard security camera system within Tioga County. |
| Status | A consistent security camera system has been implemented throughout all buildings (except Public Safety) with existing security camera systems. Additional security camera systems have been installed in other areas within the County and Shared Service entities. Each of these systems use the same ecosystem as the access control systems and provide a centrally managed platform for each building. |
| Action Item | Complete an annual penetration test to ensure the external perimeter maintains an acceptable cyber security stance. |
| | |

| | |
|---|---|
| Status | Penetration testing has been completed in two of the last three years, by two different cyber security organizations. Funding has been requested in the IT Capital project budget plan for annual penetration testing in the future. |
| Defined Goal Number Three:<br><br>Introduce and maintain transparency and accountability throughout all Tioga County ITCS services and support. | |
| Action Item | Develop and maintain documentation and diagrams for all Tioga County networks and systems. |
| Status | Several portions of the Tioga County network have been property investigated and documented.<br><br>Additional staff members have been added with the skillsets required to continue with this action item. This, along with the implementation of proper Change Management (CM) and alignment with NIST 800-53 standards, will provide a framework to follow as this action item progresses. |
| Action Item | Develop, implement and maintain a Privileged Account Authorization (PAA) process which is reviewed annually. |
| Status | This action item will be implemented with the continued alignment with NIST 800-53 frameworks. It is not currently implemented. |
| Action Item | Develop detailed and robust Change Management (CM) policies and procedures aimed at improving communication and decreasing unplanned user impact regarding required updates and changes to Tioga County networks and systems. |
| Status | In addition to the ticket management system provided by the new Tioga County Service Center (TCSC), it includes a Change Management (CM) platform. The CM platform will be used by ITCS staff to request, approve, track, and document all IT changes throughout the Tioga County infrastructure.<br><br>A Change Advisory Board (CAB) has been identified and will begin meeting weekly to complete the vetting process for all IT changes, starting in January 2025.<br><br>All upcoming changes will be communicated using the IT Service Status Board, also located in the Tioga County Service Center (TCSC). |
| Action Item | Investigate and implement a hardware and software discovery and reporting tool for all Tioga County networks and systems. |
| Status | In addition to the functionality already discussed regarding the NinjaOne RMM platform, it also provides a detailed list of software installed on each device as well as the hardware of those devices.<br><br>This does not cover hardware connected to the network that is not enrolled in the RMM, however it does partly satisfy this action item. Additional tools and systems are required to fully satisfy this requirement. |
| Action Item | Ensure all Tioga County users complete annual Cyber Security Training. |
| Status | The ITCS Department ensures all users complete the annual Cyber Security training. Various delivery methods are provided, including in-person training opportunities. |

| | |
|---|---|
| REFERRED TO: | ITCS COMMITTEE<br>LEGISLATIVE WORKSESSION |
| RESOLUTION NO. -24 | AUTHORIZE AGREEMENT WITH<br>SOUTHERN TIER NETWORK FOR<br>DARK FIBER STRANDS |

WHEREAS: The Chief Information Officer has determined existing dark fiber strands between the Tioga County Public Safety Building and the Tioga County Health and Human Services Building needs upgrading; and

WHEREAS: The Chief Information Officer has determined the existing demarcation location within the Tioga County Health and Human Services Building is insufficient for continued operational services; and

WHEREAS: The Chief Information Officer has contacted Southern Tier Network to provide dark fiber optic services between the Tioga County Public Safety Building and the Tioga County Health and Human Services Building; and

WHEREAS: The Chief Information Officer has determined increased dark fiber strands between the Tioga County Public Safety Building and the Tioga County Health and Human Services Building are necessary to complete portions of the Tioga County Public Safety Communications upgrade; and

WHEREAS: Southern Tier Network has offered to provide six (6) dark fiber strands between the Tioga County Public Safety Building and the Tioga County Health and Human Services Building for zero cost to Tioga County; therefore be it

RESOLVED: That the Chair of the County Legislature is authorized to execute this agreement between Tioga County and Southern Tier Network for six (6) dark fiber strands between the Tioga County Public Safety Building and the Tioga County Health and Human Service Building, contingent upon review and approval of the County Attorney.

REFERRED TO: ITCS COMMITTEE
LEGISLATIVE WORKSESSION

RESOLUTION NO. -24 AMEND EMPLOYEE HANDBOOK; SECTION VIII: COMPREHENSIVE INFORMATION SECURITY POLICY

WHEREAS: The Chief Information Officer and Deputy Director of ITCS have determined that aligning with the National Institute of Standards and Technology standards is appropriate for the Information Technology infrastructure within Tioga County, New York; and

WHEREAS: The Chief Information Officer and Deputy Director of ITCS have reviewed the County's Comprehensive Information Security Policy and made recommendations to remove sections IV-D. and VI-A-3 and add new Sections VI-Q-S; therefore be it

RESOLVED: That the Comprehensive Information Security Policy, Sections IV-D and VI-A-3 be removed and new Section VI-Q-S be added as follows:

**Q. Configuration Management**

**II. Purpose**

To ensure that Information Technology (IT) resources are inventoried and configured in compliance with IT security policies, standards, and procedures.

**III. Reference**

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Configuration Management (CM)

**IV. Policy**

This policy is applicable to all departments and users of Tioga County IT resources and assets.

1. Baseline Configuration

   ITCS Department shall:

   a. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.

   b. Review and update the baseline configuration of the information system annually.

   c. Review and update the baseline configuration of the information system when required as an integral part of information system component installations and upgrades.

d. Retain one previous version of baseline configurations of information systems to support rollback.

2. Configuration Change Control

   ITCS Department shall:

   a. Determine the types of changes to the information system that are configuration controlled.

   b. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.

   c. Document configuration change decisions associated with the information system.

   d. Implement approved configuration-controlled changes to the information system.

   e. Retain records of configuration-controlled changes to the information system for one year.

   f. Audit and review activities associated with configuration-controlled changes to the information system.

   g. Coordinate and provide oversight for configuration control activities through a change approval board (CAB) that convenes weekly.

   h. Test, validate, and document changes to the information system before implementing the changes on the operational system.

3. Security Impact Analysis

   ITCS Department shall:

   a. Analyze changes to the information system to determine potential security impacts prior to change implementation.

4. Access Restrictions for Change

   ITCS Department shall:

   a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

5. Configuration Settings

   ITCS Department shall:

   a. Establish and document configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements.

   b. Implement the configuration settings.

   c. Identify, document, and approve any deviations from established configuration settings.

   d. Monitor and control changes to the configuration settings in accordance with policies and procedures.

6. Least Functionality

   ITCS Department shall:

   a. Configure the information system to provide only essential capabilities.

   b. Review the information system quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services.

   c. Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.

   d. Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.

   e. Identify software programs not authorized to execute on information systems.

   f. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

   g. Review and update the list of unauthorized software programs annually.

7. Information System Component Inventory

   ITCS Department shall:

   a. Develop and document an inventory of information system components that:

      i. Reflects the current information system accurately.

ii. Includes all components within the authorization boundary of the information system.

iii. Is at the level of granularity deemed necessary for tracking and reporting.

iv. Includes information deemed necessary to achieve effective information system component accountability.

b. Review and update the information system component inventory annually.

c. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.

d. Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the information system.

e. Take the following actions when unauthorized components are detected:

i. Disable network access by such components, or

ii. Isolate the components and notify the Chief Information Officer and system owner.

f. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

8. Configuration Management Plan

ITCS shall develop, document, and implement a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures.

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.

c. Defines the configuration items for the information system and places the configuration items under configuration management.

d. Protects the configuration management plan from unauthorized disclosure and modification.

9. Software Usage Restrictions

   ITCS Department shall:

   a. Use software and associated documentation in accordance with contract agreements and copyright laws.

   b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

   c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not sued for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

10. User Installed Software

    ITCS Department shall:

    a. Establish policies governing the installation of software by users.

    b. Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.

    c. Monitor policy compliance quarterly.

### V. Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

### VI. Policy Exceptions

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) and the Information Security Officer (ISO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

## R. Contingency Planning

### II. Purpose

To ensure that Information Technology (IT) resources are available during times of disruption of services.

## III. Reference

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Contingency Planning (CP), NIST SP 800-16, NIST SP 800-34, NIST SP 800-50, NIST 800-84; NIST Federal Information Processing Standards (FIPS) 199

## IV. Policy

This policy is applicable to all departments and users of Tioga County IT resources and assets.

1. Contingency Plan

   ITCS Department shall:

   a. Develop a contingency plan for the information system, in direct guidance and association with the information system owner, that:

      i. Identifies essential missions and business functions and associated contingency requirements.

      ii. Provides recovery objectives, restoration priorities, and metrics.

      iii. Addresses contingency roles, responsibilities, assigned individuals with contact information.

      iv. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.

      v. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

      vi. Is reviewed and approved by the Chief Information Officer, and information system's owner management on at least an annual basis.

   b. Distribute copies of contingency plans to key contingency personnel, identified by name and/or by business role.

   c. Coordinate contingency planning activities with incident handling activities.

   d. Update the contingency plan to address changes to the business owner's mission, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

   e. Communicate contingency plan changes to key contingency personnel identified by name and/or by business role.

f. Protect the contingency plan from unauthorized disclosure and modification.

2. Contingency Training

   ITCS Department shall:

   a. Provide contingency training to information system users consistent with assigned roles and responsibilities.

   b. Ensure designated personnel receive contingency training at least biannually of assuming a contingency role or responsibility, and when required by information system changes.

3. Contingency Plan Testing

   ITCS, along with information system owners, shall:

   a. Test the contingency plan for the information system, as determined by the mission critical nature of the business system(s) no less than annually.

   b. Use strategic and tactical planning during testing to simulate a production information system to determine the effectiveness of the plan and the organizational readiness to execute the plan.

   c. Review the contingency plan test results.

   d. Initiate corrective actions, as needed.

   e. Coordinate contingency plan testing with organizational elements responsible for related plans; plans related to contingency plans for information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans.

4. Alternate Storage Site

   ITCS, in direct guidance and association with the information system owner, shall:

   a. Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.

   b. Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

   c. Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

d. Identify and document potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

5. Alternate Processing Site

   ITCS, in direct guidance and association with the information system owner, shall:

   a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of the information system operations for essential missions/business functions within the time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable.

   b. Ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the agreed upon time period for transfer/resumption.

   c. Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site.

   d. Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

   e. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

   f. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with business objectives and availability requirements.

6. Telecommunications Services

   ITCS Department shall:

   a. Establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within agreed upon recovery timeframes when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

   b. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with agreed upon recovery objectives and availability requirements.

c. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

7. Information System Backup

   ITCS, in direct guidance and association with the system owner, shall:

   a. Conduct backups of user-level information contained in the information system defined by frequency consistent with recovery time and recovery point objectives.

   b. Conduct backups of system-level information contained in the information system defined by frequency consistent with recovery time and recovery point objectives.

   c. Conduct backups of information system documentation including security-related documentation defined by frequency consistent with recovery time and recovery point objectives.

   d. Protect the confidentiality, integrity, and availability of backup information at storage locations.

   e. Test backup information to verify media reliability and information integrity.

8. Information System Recovery and Reconstitution

   ITCS, in direct guidance and association with the information system owner, shall:

   a. Provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

   b. Provide that the information system implements transaction recovery for systems that are transaction-based.

**V. Compliance**

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

## VI. Policy Exceptions

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) and the Information Security Officer (ISO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

## S. Identification and Authentication

### II. Purpose

To ensure that only properly identified and authenticated users and devices are granted access to Information Technology (IT) resources in compliance with IT security policies, standards, and procedures.

### III. Reference

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST 800-76, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100, NIST SP 800-116; Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors; NIST Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140

### IV. Policy

This policy is applicable to all departments and users of Tioga County IT resources and assets.

1. Identification and Authentication

   ITCS Department shall:

   a. Ensure that information systems uniquely identify and authenticate users or processes acting on behalf or Tioga County users.

   b. Ensure that information systems implement multifactor authentication for network access to privileged accounts.

   c. Ensure that information systems implement multifactor authentication for network access to non-privileged accounts.

   d. Ensure that information systems implement multifactor authentication for local access to privileged accounts.

e. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.

f. Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

2. Device Identification and Authentication

   ITCS Department shall:

   a. Ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.

3. Identifier Management

   ITCS Department, through department information systems owners, shall:

   a. Ensure that Tioga County, NY manages information system identifiers by receiving authorization from the Chief Information Officer to assign an individual, group, role, or device identifier.

   b. Select an identifier that identifies an individual, group, role, or device.

   c. Assign the identifier to the intended individual, group, role, or device.

   d. Prevent reuse of identifiers for 90 days.

   e. Disable the identifier after 60 days of inactivity.

4. Authenticator Management

   ITCS Department shall:

   a. Ensure that information systems, for password-based authentication, enforce minimum password complexity that must not contain the user's entire Account Name value, entire Full Name value or any Personally Identifiable Information (PII).

   b. Ensure passwords must contain characters from three of the following five categories:

      i. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);

      ii. Lowercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);

      iii. Base 10 digits (0 through 9);

iv. Non-alphanumeric characters ~!@#$%^&  -+=|\(){}[]::'"<>,.?/; and

v. Any Unicode character that is categorized as an alphanumeric character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

c. Require passwords to have a minimum length of 8 characters.

d. Enforce at least one changed character when new passwords are created.

e. Store and transmit only cryptographically protected passwords.

f. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.

g. Prohibit password reuse for 12 generations.

h. Allow the use of a temporary password for system logons with an immediate change to a permanent password.

i. Require that the registration process to receive authenticators be conducted in person or by a trusted third party with authorization by the Chief Information Officer.

**V. Compliance**

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

**VI. Policy Exceptions**

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) and the Information Security Officer (ISO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.