



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



INFORMATION TECHNOLOGY LEGISLATIVE STANDING COMMITTEE

November 5th, 2024, at 9:30 am

ATTENDANCE:

- Legislators: Jake Brown, Tracy Monell, Dennis Mullen, Ron Ciotoli, William Standing, 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.

- 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.

Review of 2024 Budget and Financial News

A1680 – Year-to-Date Budget Report

FOR 2024 12									
ACCOUNTS FOR:		ORIGINAL	TRANFRS/	REVISED	YTD	ENCUMBRANCES	AVAILABLE	PCT	
A	General Fund	APPROP	ADJSTMTS	BUDGET	ACTUAL		BUDGET	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	TRANFRS/	REVISED	YTD	ENCUMBRANCES	AVAILABLE	PCT
		APPROP	ADJSTMTS	BUDGET	ACTUAL		BUDGET	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:	ORIGINAL	TRANFRS/	REVISED	YTD	ACTUAL	ENCUMBRANCES	AVAILABLE	PCT
H Capital Fund	APPROP	ADJSTMTS	BUDGET				BUDGET	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	TRANFRS/	REVISED	YTD	ACTUAL	ENCUMBRANCES	AVAILABLE	PCT
	APPROP	ADJSTMTS	BUDGET				BUDGET	USE/COL
GRAND TOTAL	244,313	214,559	458,872	361,151.34		21,837.50	75,882.96	83.5%

REFERRED TO:

ITCS COMMITTEE
LEGISLATIVE WORKSESSION

RESOLUTION NO. -24

AUTHORIZE AGREEMENT WITH
SOUTHERN TIER NETWORK FOR
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 of 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.