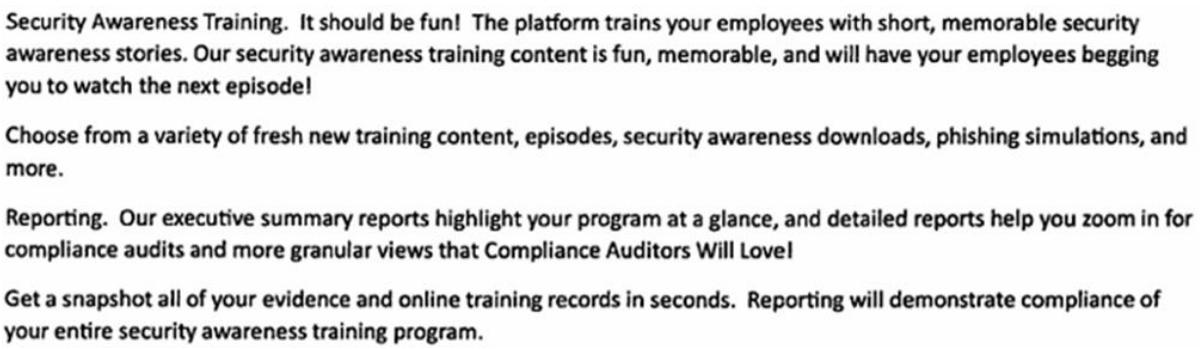
Current IT Agreement

The current IT agreement provides for the day to day operation of the IT infrastructure and security for the city. The cyber security portion of this provides additional security tools and monitoring for the city. This includes:

- Technical security controls
- Security process to help keep environment secure on a daily basis
- Monitor and remediate issues in the environment
- Proactive, persistent threat protection for your network that identifies vulnerabilities and allows earlier detection of ransomware activity
- Integris uses state-of-the-art security tools that can detect various Indications of compromise (IOC) on computers or servers in the network



Security Awareness Training. It should be fun! The platform trains your employees with short, memorable security awareness stories. Our security awareness training content is fun, memorable, and will have your employees begging you to watch the next episode!

Choose from a variety of fresh new training content, episodes, security awareness downloads, phishing simulations, and more.

Reporting. Our executive summary reports highlight your program at a glance, and detailed reports help you zoom in for compliance audits and more granular views that Compliance Auditors Will Love!

Get a snapshot all of your evidence and online training records in seconds. Reporting will demonstrate compliance of your entire security awareness training program.

vCISO Project

The vCISO project is designed to guide the city in establishing and maintaining the management controls needed to meet the Sate Cybersecurity Act

- Compliance is a governance function (GRC - Governance, Regulation and Compliance)
- Implements Managerial Security controls
- Confirm that technical controls (as performed by the base IT and security agreement) needed by the State are also reviewed and confirmed for that section of the statute
- Building a portal that can then be run by the City to maintain compliance – currently under production- I can share at our next one-on-one meeting as well as at the next Commission Workshop on July 23, 2025.

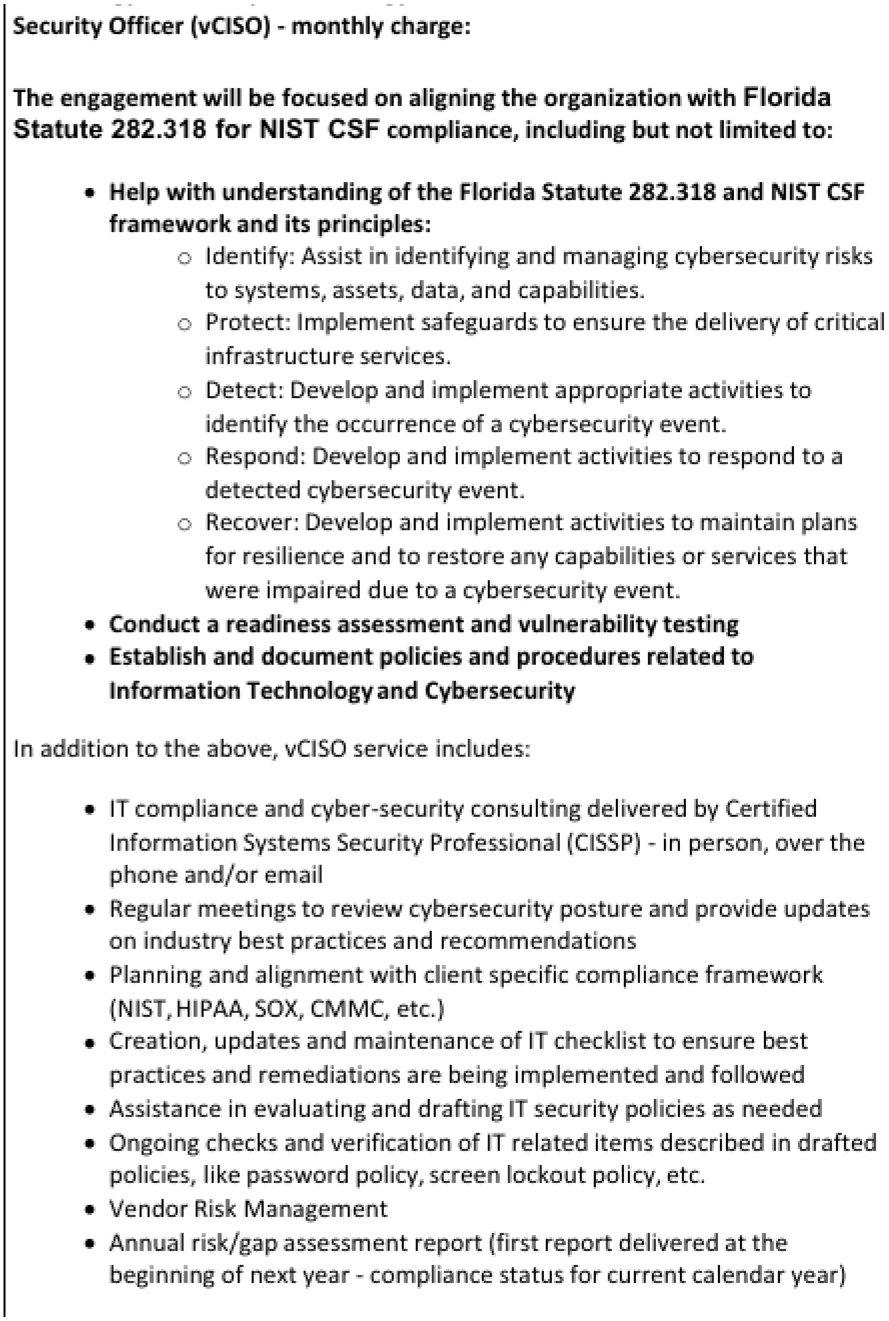
The State Statute requires procedures and policies be put in place for security management

- Goal to ensure entire standard is being followed
- Includes procedures for Incident Response and Management
- Guidance to make sure we are setting up the procedures and measures the state is looking for to be compliant

Here are some key paragraphs from the statute.
Chapter 282 Section 318 - 2024 Florida Statutes

- Failure to report cybersecurity incidents: governments required to report ransomware incidents and any cybersecurity incident of severity level 3, 4, or 5 to the Cybersecurity Operations Center and the Cybercrime Office of the Department of Law Enforcement. Failure to do so could result in accountability and potential consequences.
- Failure to implement cybersecurity standards: governments are required to implement managerial, operational, and technical safeguards to protect government data and information technology resources, aligning with risk management strategies. Non-compliance with these requirements could lead to investigations and potential disciplinary action.

- Impact on public health, safety, and security: Incidents of severity levels 3, 4, and 5 can have a demonstrable impact on public health, safety, economic security, and civil liberties. Negligence or non-compliance leading to such incidents could result in severe consequences.



Security Officer (vCISO) - monthly charge:

The engagement will be focused on aligning the organization with Florida Statute 282.318 for NIST CSF compliance, including but not limited to:

- **Help with understanding of the Florida Statute 282.318 and NIST CSF framework and its principles:**
  - Identify: Assist in identifying and managing cybersecurity risks to systems, assets, data, and capabilities.
  - Protect: Implement safeguards to ensure the delivery of critical infrastructure services.
  - Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
  - Respond: Develop and implement activities to respond to a detected cybersecurity event.
  - Recover: Develop and implement activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
- **Conduct a readiness assessment and vulnerability testing**
- **Establish and document policies and procedures related to Information Technology and Cybersecurity**

In addition to the above, vCISO service includes:

- IT compliance and cyber-security consulting delivered by Certified Information Systems Security Professional (CISSP) - in person, over the phone and/or email
- Regular meetings to review cybersecurity posture and provide updates on industry best practices and recommendations
- Planning and alignment with client specific compliance framework (NIST, HIPAA, SOX, CMMC, etc.)
- Creation, updates and maintenance of IT checklist to ensure best practices and remediations are being implemented and followed
- Assistance in evaluating and drafting IT security policies as needed
- Ongoing checks and verification of IT related items described in drafted policies, like password policy, screen lockout policy, etc.
- Vendor Risk Management
- Annual risk/gap assessment report (first report delivered at the beginning of next year - compliance status for current calendar year)