Cybersecurity Plan 2026-2028

Vision:

To maintain a resilient, AI-fortified digital ecosystem that ensures the safety of Lincolnton's citizens and the continuity of municipal services against increasingly sophisticated global threats.

Mission:

Safeguard city data through Zero Trust principles, leverage Agentic AI for rapid incident response, and cultivate a "Human-AI" workforce prepared for the next generation of social engineering.

Roadmap Elements: 2026–2028

1. Advanced Human Risk Management (Knowbe4 Evolution)

    As phishing becomes hyper-personalized through AI deepfakes, training must move beyond basic videos.

    AI Defense Training: Implement modules specifically for identifying AI-generated voice and video (Deepfakes).

    PhishER Plus Integration: Automate the "Phish Alert" pipeline to remove reported threats from all city inboxes instantly using AI-driven orchestration.

    Human-Agent Coaching: Train staff on the responsible use of AI tools and how to secure "non-human identities" like API keys.

2. Zero Trust & Network Evolution (Cisco/Meraki)

Moving toward the Cisco Meraki for Government framework to ensure FedRAMP-level compliance and "Never Trust, Always Verify" access.

- Micro-Segmentation: Isolate SCADA (Water/Power) and Public Safety networks from administrative traffic so a breach in one department cannot spread.
- Identity-First Access: Transition from simple MFA to "Passwordless" authentication and device-bound credentials for all users.
- Unified SASE: Consolidate Cisco Umbrella and AnyConnect into a single Secure Access Service Edge (SASE) for seamless security whether staff are at City Hall or in the field.

3. AI-Driven Security Operations (SecOps)

The 2028 goal is to reduce the Mean Time to Respond (MTTR) by at least 30% through automation.

- Autonomous Threat Hunting: Deploy AI agents that scan for "Shadow IT" (unauthorized devices) and unusual traffic patterns in real-time.
- Self-Healing Infrastructure: Implement protocols where the network can automatically isolate a compromised workstation before a human technician even sees the alert.

Funding & Sustainability

Lincolnton will continue to leverage the General Fund and Enterprise Funds, but will now prioritize:

- SLCGP Grants: Actively pursuing the reauthorized State and Local Cybersecurity Grant Program, which now includes specific funding for AI systems and Operational Technology (OT) through 2033.
- Insurance Optimization: Modernizing to Zero Trust to lower annual cyber insurance premiums.

2028 Pricing & Lifecycle Projections

Phishing and Training Platform-PHISH ER-

Knowbe4

Yearly ($6,000)

Infrastructure Networking / Server

Meraki/Nutanix

Yearly ($107,000)

Multi-Factor Authentication

Cisco Duo

Yearly ($7,000)

Cloud DNS-XDR- Internal managed SOC

Cisco Umbrella, AnyConnect

Yearly ($35,000)

Totals

Yearly ($155,000)

Cybersecurity Program Goals and Objectives:

Enhance Preparedness & AI Resilience

The City of Lincolnton is evolving its strategy to address the era of generative threats by transitioning from basic awareness to advanced Human Risk Management. We are implementing specialized training modules to help end users identify AI-generated deepfakes and hyper-personalized social engineering. We continue to conduct randomized phishing exercises, now enhanced with AI-driven orchestration that can automatically retract reported threats from all city inboxes in real-time. Additionally, we provide advanced coaching on the secure use of AI tools to prevent the accidental exposure of city data.

Assessment and Autonomous Mitigation

The City has expanded its arsenal of tools to include Agentic AI for proactive threat hunting and rapid incident response. Our infrastructure now utilizes firewall and switch gear capable of identifying threats at the machine level, supplemented by autonomous agents that can isolate compromised devices in milliseconds. Our cloud email security has been upgraded to scan for AI-authored malware and sophisticated spoofing attempts. With the integration of a unified Secure Access Service Edge (SASE) and cloud DNS, we ensure users remain protected against hijacking and interference whether they are working on-site or remotely.

Manage, Monitor, and Orchestrate

Building on our previous hyperconvergence overhaul, the City of Lincolnton is moving toward a Zero Trust Architecture to manage all virtual and physical assets. We have implemented network micro-segmentation, isolating SCADA and Emergency Services from administrative traffic to ensure a breach in one department cannot spread. We continuously monitor the health of our Google Workspace and cloud environments with an in-depth, AI-powered look at all data traversing the network. By the end of this roadmap, the City will have the capability to not only track threats but to deploy self-healing protocols that automatically remediate vulnerabilities before they can be exploited.

Monitor, Audit, and Automated Recovery

With the 2028 initiatives, the City of Lincolnton has the ability to monitor all internal and external traffic with enhanced visibility into non-human identities and API connections. Our cloud platforms offer granular reporting on resource usage, access permissions, and automated compliance auditing. We track incremental changes in all city resources using

immutable backups, which facilitates the rapid reconstruction of data and ensures continuity of operations in the event of a sophisticated cyberattack.

Best Practices and Methodologies

- Implement Zero Trust Authentication: Transitioning from standard multi-factor authentication to identity-first, passwordless access for users with mission-critical data, including financials, employee information, and case files.
- Next-Gen Human Risk Training: Deploying an evolved training platform that tests skills against AI-driven threats, including monthly deepfake awareness and PhishER automated remediation initiatives.
- Micro-Segmentation and Cloud Backbone: Encrypting and limiting access to infrastructure through network micro-segmentation, securing information via a cloud DNS backbone (Cisco Umbrella) that remains active on city-owned devices off-premise.
- Autonomous Device Management: Utilizing mobile device managers to facilitate software pushes and configurations that safeguard devices both on and off-premise.
- Automated Lifecycle Maintenance: Keeping operating systems and anti-virus up to date by deploying zero-day and security patches automatically in accordance with vendor specifications for our Nutanix and Windows Server platforms.
- Security Validation: Moving beyond yearly penetration testing to more frequent, automated security validations to safeguard against rapid threat evolution and reinforce our deployments.

Continuity of Operations

The City of Lincolnton has built infrastructure systems to be agile in the event of an attack, utilizing self-healing protocols that allow us to pivot from on-premise to remote cloud-hosted systems with maximum flexibility. While the following steps are tailored to specific threat situations, our priority is to restore connectivity and isolate threats using the order established below:

- Identify the threat using autonomous monitoring tools.
- Eliminate and limit contact with threats or affected systems via automated network isolation.
- Deploy clean machines and secure virtual environments to conduct daily business.

Departments to be restored in priority order:

- SCADA Systems: Water/Wastewater.
- Emergency Services: Police/Fire.
- Utility & Customer Engagement: Electric and Utility Billing.
- Administrative Operations: HR, Finance, CMO, and Planning.
- Community Services: Parks and Recreation

Following restoration, we build an investigation into the threat origination, reporting findings through proper channels and alerting authorities as warranted.

_____	_____
Chris Jones	Ed Hatley, Mayor
City of Lincolnton	City of Lincolnton
Technology & Innovation	Lincolnton, City Council