FLORIDA ASSOCIATION OF COUNTIES TRUST

FLGISA
LEADERSHIP • INNOVATION • COLLABORATION

Cybersecurity & Emerging Technology:

PREPARING COUNTIES FOR WHAT'S NEXT

67 Counties. 67 Communities.

ONE FLORIDA

CYBERSECURITY MISCONCEPTIONS. REAL OPERATIONAL RISK.

Misconceptions create blind spots. Blind spots create risk.
The impact goes beyond IT—it affects our mission and our community.

COMMON MISCONCEPTIONS

WE WON'T BE TARGETED.

Attackers target all organizations—large and small.

OUR EMAIL FILTER WILL CATCH IT.

Filters aren't perfect. People are still the #1 target.

WE HAVE ANTIVIRUS, SO WE'RE SAFE.

Antivirus is just one layer. Modern attacks can go undetected.

IT WILL HANDLE IT.

Cybersecurity is everyone's responsibility. We all play a role.

OUR DATA IS IN THE CLOUD, SO IT'S SECURE.

The cloud is secure, but our settings and behavior matter.

HOW MISCONCEPTIONS CREATE OPERATIONAL RISK

- Higher chance of successful attacks
- System outages and service interruptions
- Financial losses and increased recovery costs
- Data loss or exposure of sensitive information
- Reduced public trust and reputational damage
- Delayed projects and mission impact

**Stay informed. Stay vigilant. Protect our systems.
Protect our mission.**

CYBERSECURITY IS OPERATIONAL INFRASTRUCTURE, NOT OPTIONAL TECHNOLOGY SPENDING.

Local leaders should think of cybersecurity like water, roads, and emergency services—essential to how we serve our communities.

THINK OF CYBERSECURITY AS...

ESSENTIAL TO EVERY SERVICE

Just like water, cybersecurity is foundational to everything we do.

BUILT FOR RELIABILITY

It keeps operations running smoothly—today and into the future.

PREPARED FOR DISRUPTION

Investing now helps us prevent, respond to, and recover from incidents.

PROTECTS OUR COMMUNITY

Strong cybersecurity safeguards services, data, and public trust.

SMART STEWARDSHIP

Proactive investment reduces risk, costs less, and delivers lasting value.

WHAT STRONG CYBERSECURITY DELIVERS

CONTINUITY
Keeps critical services available when we need them most.

RESILIENCE
Reduces downtime and speeds recovery from disruptions.

EFFICIENCY
Protects systems so staff can focus on serving residents.

TRUST
Demonstrates responsible leadership and protects public confidence.

VALUE
Prevents costly incidents and supports long-term financial health.

Cybersecurity isn't optional.
It's how we keep our community safe, our services running, and our future strong.

Information Technology Stack Framework

Information Technology Stack

Regulatory & National Frameworks, Standards

REGULATORY: (Federal Laws, State Statutes)

FEDERAL

- HIPAA
- FISMA
- GLBA
- PCI-DSS
- EO-Cyber
- NIST SP800-53 Rev.5
- CIRCIA
- FOIA
- GDPR

ADA (Title II, WCAG 2.X)

FLORIDA

- PRR Chapter 119 (119.0725)
- FL Stat. Sections 281.301
- FL Stat. 282.318
- FL Stat. 282.3185
- FL Stat. 282.3186

NATIONAL FRAMEWORKS, STANDARDS

- NIST (National Institute of Standards) CSF (Cybersecurity Framework) or MITRE
- CIS Controls
- SOC2
- PCI-DSS
- HITRUST (CSF)

Information Technology Stack

MISSION STATEMENT

Serving Our Community to Create a Better Future

CORE VALUES

- Integrity
- Respect
- Service Excellence
- Innovation

Organizational Policies

- Administrative Policy
- Personnel Policy and Procedure Manual
- Security Policy
- AI Policy
- Reliance Cyber Policy (Gallagher Insurance)

Baseline Monitoring of the IT Stack

01

Annual Security Assessment
(County and 6th Judicial Court Network)

02

Annual PCI-DSS Audit

03

Annual County Audit
(Through the IG Office, Clerk of the Court & Comptroller)

04

Reliance Edge Appliance, 24/7 Security monitoring

05

Security Operation Center (SOC) monitoring 24 x 7

06

Weekly / Monthly IT Self-Assessment and NIST Heat Map status

Proactive Monitoring. Continuous Assurance. Stronger Security.

FLORIDA STATUTE 119.0725
WHAT IT MEANS FOR LOCAL GOVERNMENTS

Strengthening cybersecurity. Protecting our community. Complying with the law.

WHAT IS FLORIDA STATUTE 119.0725?

Florida Statute 119.0725, **Florida Digital Service Act**, establishes cybersecurity requirements for state agencies and, by extension, requires local governments that connect to or use state digital services to maintain appropriate cybersecurity practices and report certain incidents.

WHO IS AFFECTED?

Counties, municipalities, special districts, school districts, and other local government entities that use, access, or connect to state digital services or transmit data as defined in the statute.

KEY REQUIREMENTS THAT APPLY TO LOCAL GOVERNMENTS

MAINTAIN CYBERSECURITY PRACTICES

Implement and maintain reasonable and appropriate cybersecurity measures.

RISK MANAGEMENT

Assess and manage risks to information systems and data.

PROTECT DATA & SYSTEMS

Protect the confidentiality, integrity, and availability of data and systems.

REPORT INCIDENTS

Report qualifying cybersecurity incidents to the Department of Management Services.

COOPERATE WITH THE STATE

Cooperate with state requests for information and incident response activities.

WHAT IS AN INCIDENT RESPONSE PLAN?

An Incident Response Plan is a documented, actionable plan that outlines for, detect, cgamation tond recover from cybersecurity incidents.

- Defines roles and responsibilities
- Identifies and contains incidents
- Eradicates threats and recovers operations
- Communicates with stakeholders and authorities
- Documents lessons learned and improves processes

HOW IT IS USED AND REPORTED

1. **DETECT & ASSESS** — Identify a potential cybersecurity incident and assess its scope and impact.
2. **ACTIVATE PLAN** — Activate the Incident Response Plan and engage the response team.
3. **CONTAIN & RESPOND** — Contain the incident, eradicate the threat, and begin recovery efforts.
4. **NOTIFY & REPORT** — Report qualifying incidents to the Department of Management Services as required by F.S. 119.0725.
5. **RECOVER & IMPROVE** — Restore normal operations, review the incident, and update the plan to strengthen defenses.

Compliance with F.S. 119.0725 helps protect our residents, our data, and our ability to deliver trusted services.

Be prepared. Have a plan. Report incidents. Strengthen our cybersecurity together.

SMART DECISIONS. STRONGER OPERATIONS.

We evaluate every option—on premise, in the cloud, with partners, and total cost—to choose what best supports our mission and community.

HOW WE MAKE TECHNOLOGY DECISIONS

HOST ON PREMISE

- Full control and customization
- Meets compliance or data residency needs
- Best for systems requiring high performance or local integration

HOST IN THE CLOUD

- Scalability and flexibility
- Fast deployment
- Lower upfront infrastructure costs

USE 3RD PARTY IT VENDOR MANAGEMENT

- Access specialized expertise
- Focus on core mission
- Share risk and improve accountability

TOTAL COST OF OWNERSHIP

- Look beyond upfront costs
- Include operations, support, security, and scalability
- Choose the best long-term value

KEY FACTORS WE CONSIDER

SECURITY & COMPLIANCE
Protecting data and meeting laws and standards.

PERFORMANCE & RELIABILITY
Ensuring systems are available, fast, and dependable.

FLEXIBILITY & SCALABILITY
Adapting to change and growing needs.

RISK & RESILIENCE
Managing risk and ensuring business continuity.

COST & VALUE
Maximizing long-term value and responsible spending.

MISSION IMPACT
Supporting better services for our community.

Every decision is mission-driven, risk-aware, and value-focused—delivering the right technology in the right way.

PATCH MANAGEMENT. PROTECT TODAY. PREVENT TOMORROW.

Patch management is the ongoing process of identifying, testing, and applying software updates—called patches—to fix vulnerabilities and improve performance.

WHAT IS PATCH MANAGEMENT?

1. IDENTIFY

Scan systems to find missing patches and vulnerabilities.

2. ASSESS

Evaluate the risk and prioritize patches that matter most.

3. TEST

Test patches in a safe environment to ensure compatibility.

4. DEPLOY

Apply approved patches to systems in a controlled, timely way.

5. MONITOR

Verify success and monitor for issues to keep systems secure.

WHY PATCH MANAGEMENT IS IMPORTANT

CLOSES SECURITY GAPS

Fixes vulnerabilities attackers could exploit.

REDUCES RISK

Lower chance of breaches, downtime, and data loss.

IMPROVES PERFORMANCE

Updates often include stability and reliability improvements.

SUPPORTS COMPLIANCE

Helps meet security standards and audit requirements.

SAVES TIME AND MONEY

Preventing issues costs less than fixing them.

PROTECTS OUR COMMUNITY

Secure systems mean reliable services for everyone.

Timely patches. Stronger defenses. Reliable services.
That's how we protect our systems and our community.

CYBER INSURANCE. FINANCIAL PROTECTION WHEN IT MATTERS MOST.

Cyber insurance helps our organization recover from cyber incidents, but making it work for us requires planning, partnership, and preparation.

THE IMPORTANCE OF CYBER INSURANCE

FINANCIAL PROTECTION
Helps cover costs from incidents, ransomware, and data breaches.

FASTER RECOVERY
Provides access to experts and resources when we need them.

RISK TRANSFER
Transfers part of the financial risk to the insurance provider.

STRONGER RESILIENCE
Encourages better security practices and preparedness.

STAKEHOLDER CONFIDENCE
Demonstrates responsible risk management to residents and leaders.

THE CHALLENGES

RISING COSTS
Premiums are increasing and deductibles are getting higher.

COMPLEX REQUIREMENTS
Applications are detailed and require significant time and documentation.

CHANGING CRITERIA
Insurers frequently update requirements and coverage expectations.

LIMITED COVERAGE
Policies have exclusions and limits—reading the fine print matters.

PREEMPTIVELY SCREEN INSURANCE PROVIDER VENDORS

Have trusted partners ready before an incident occurs.

PUBLIC RELATIONS SERVICES
- Protects our reputation
- Pre-approved messaging
- Experienced in crisis communication
- Understands our community

LEGAL SERVICES
- Expert guidance on laws and regulations
- Data breach and privacy expertise
- Contract and liability support
- Protects our rights and interests

RECOVERY SERVICES
- Incident response and forensics
- System restoration and data recovery
- Business continuity support
- Minimizes downtime and disruption

Cyber insurance is more than a policy—it's a partnership.
Plan ahead. Vet vendors. Strengthen our recovery.

PREPARE | PARTNER | PROTECT

EMERGING TECHNOLOGIES (INCLUDING AI). PREPARE TODAY. LEAD TOMORROW.

Emerging technologies can transform how we serve our community.
Planning proactively ensures we stay current, competitive, and effective.

WHY EMERGING TECHNOLOGIES MATTER

IMPROVE SERVICE DELIVERY

Streamline processes and deliver faster, smarter services.

ENHANCE DECISION MAKING

Use data and AI insights to make better, faster, data-informed decisions.

STRENGTHEN RESILIENCE

Anticipate challenges, detect threats earlier, and respond effectively.

EMPOWER OUR PEOPLE

Equip staff with modern tools to be more productive and innovative.

DRIVE LONG-TERM VALUE

Invest in technologies that deliver value and reduce future costs.

STAY COMPETITIVE AND RELEVANT

Keep pace with changing needs and rising community expectations.

PLAN PROACTIVELY FOR THE NEXT 3–5 YEARS

1. ASSESS FUTURE NEEDS

Identify emerging trends, community needs, and technology opportunities.

2. BUILD A STRATEGIC ROADMAP

Prioritize investments that align with our mission, resources, and long-term goals.

3. PILOT AND LEARN

Test new technologies in low-risk ways and measure real impact.

4. INVEST WISELY

Focus on solutions that are secure, scalable, and deliver measurable outcomes.

5. ADAPT AND EVOLVE

Continuously review, learn, and adjust to stay current and future-ready.

Emerging technologies are not just about today—
they are about building a stronger, smarter future for our community.
Plan ahead. Invest wisely. Lead with purpose.

INNOVATE | SECURE | SERVE

WHAT KEEPS LOCAL GOVERNMENT LEADERS UP AT NIGHT—AND HOW WE STAY AHEAD.

Cyber threats don't take nights off.
Proactive leadership today protects our services, our people, and our future.

WHAT KEEPS YOU UP AT NIGHT

CYBERATTACKS & DATA BREACHES

Ransomware, phishing, and breaches can disrupt services and expose sensitive data.

DOWNTIME & SERVICE DISRUPTIONS

Outages impact public safety, operations, and resident trust.

COMPLIANCE & REGULATORY RISK

Evolving laws and standards create pressure—and penalties—if we fall short.

BUDGET & RESOURCE CONSTRAINTS

Limited budgets and staffing make it hard to keep up with growing risks.

THIRD-PARTY & SUPPLY CHAIN RISK

Vendors and partners can introduce vulnerabilities beyond our control.

REPUTATION & PUBLIC TRUST

Incidents damage confidence and can take years to recover from.

HOW WE STAY AHEAD: LEADER PRIORITIES

1. STRENGTHEN THE FOUNDATION

- Maintain core systems (Oracle, Accela, CAD, Microsoft Office)
- Keep systems stable, patched, and secure
- Follow proven cybersecurity practices

2. PLAN & INVEST PROACTIVELY

- Build a 3–5 year technology and cybersecurity roadmap
- Evaluate emerging technologies (including AI)
- Align investments with mission and budget

3. MANAGE RISK HOLISTICALLY

- Assess risks across people, processes, and technology
- Manage third-party vendors and contracts
- Maintain strong access controls and data protection

4. PREPARE & TEST OFTEN

- Test and update incident response plans
- Conduct regular backups and recovery testing
- Partner with insurance, legal, PR & recovery experts

5. EMPOWER OUR PEOPLE

- Provide ongoing security awareness training
- Promote a culture of vigilance and accountability
- Ensure clear roles and communication

6. MEASURE & IMPROVE

- Track key metrics and performance
- Continuously evaluate and adapt
- Report and communicate progress

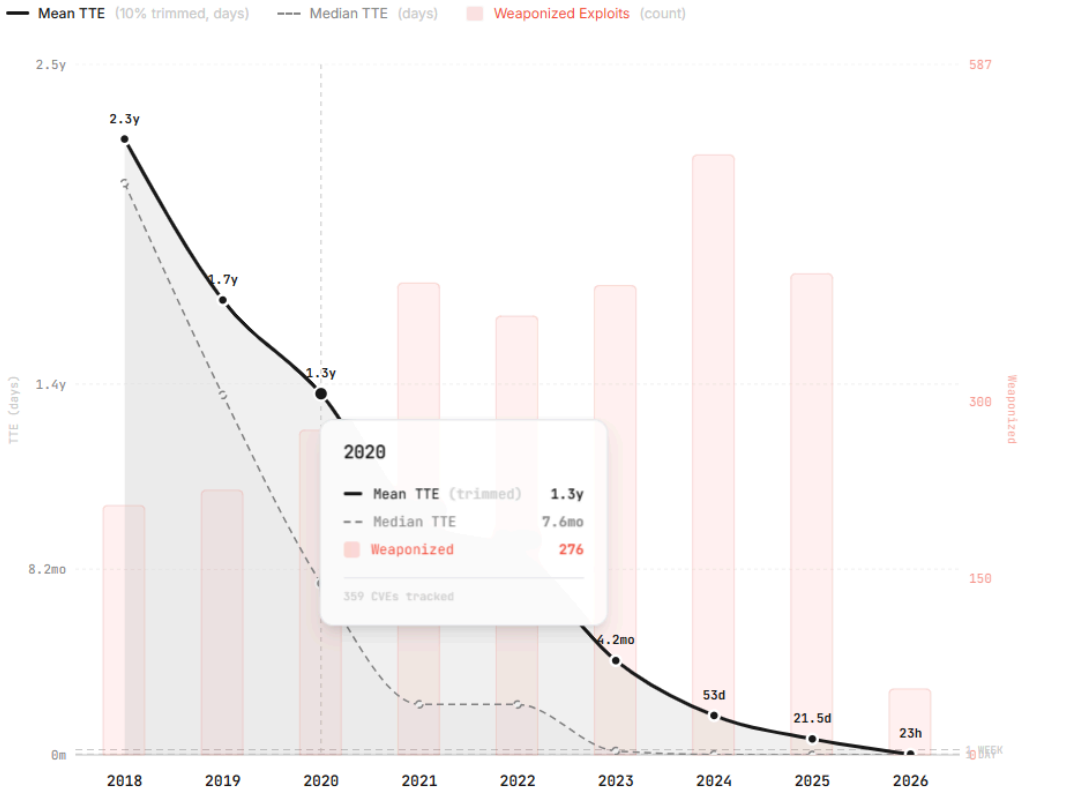
Proactive leadership today builds a safer, smarter, and more resilient community.
Prioritize. Prepare. Protect. That's how we keep our community moving forward.

SECURE SYSTEMS | RESILIENT STAFF | TRUSTED SERVICES | STRONG COMMUNITY

OUR MISSION. OUR COMMUNITY. OUR RESPONSIBILITY.

From Vulnerability to Exploitation

TTE measures the gap between CVE public disclosure and first confirmed in-the-wild exploitation. Zero = same-day.



Based on 3,500+ confirmed-exploited CVEs (CISA KEV + VulnCheck KEV, with VulnCheck XDB timestamps for early-year CVEs)

zerodayclock.com

Time-to-Exploit Milestones

Projected year when median TTE crosses each threshold — extrapolated from observed 2018–2024 trend

1 Year	1 Month	1 Week	1 Day	1 Hour	1 Minute
REACHED	REACHED	REACHED	REACHED	PROJECTED	PROJECTED
~2021	~2025	~2026	~2026	~2027	~2027

FLORIDA ASSOCIATION OF COUNTIES TRUST

FLGISA
LEADERSHIP • INNOVATION • COLLABORATION

OUR MISSION
OUR COMMUNITY
OUR RESPONSABILITY

67 Counties. 67 Communities.
ONE FLORIDA