Steps to secure the network

Strong Wi-Fi Password	Change the default password to a unique, complex one
Enable Encryption	Use WPA3 or WPA2 for secure Wi-Fi.
Update Firmware	Regularly update your router’s firmware for security patches.
Use Newer Hardware	Upgrade to a modern router/modem for better security and performance.
Create a Guest Network	Isolate guest users to prevent access to your main network.
Secure IoT Devices	Use strong, unique passwords and update firmware regularly
Enable Firewall	Configure your router's firewall to block unwanted traffic

Classified vs. Public Data

Sensitive/Classified	Public
PII, health, financial, legal docs, trade secrets.	Newsletters, Public flyers.

Rule: *If unsure, treat as sensitive.*

Urgent vs. Non-Urgent (Florida Law §282.3185)

Level	State	Report Within
Emergency	Ransomware disabling emergency services	12 hours
Severe	Large-scale data exposure	48 hours
High	Credential theft, DoS attack	48 hours
Medium	Suspicious but contained	Report IT
Low	minimal risk (forgotten password, scan alerts)	Report IT

Incident Detection and Response

In the context of cybersecurity, an incident is an abnormal event that might impact an organization's or agency's normal operations.

Cybersecurity Awareness

We must all learn about cybersecurity to protect ourselves and our agencies. Continuous education on cyber threats, risks, and best practices is essential.
We all have a responsibility to learn about emerging threats. By doing so, we can:
1) Prevent incidents proactively
2) Identify vulnerabilities in systems
3) Adapt training, plans, and policies as needed

Firewall

Firewalls are barriers between trusted networks and untrusted networks.
Firewall rules:
1) Deny traffic from certain network addresses or geographic regions
2) Deny services, ports, and applications
3) Allow traffic from trusted networks

Data backup

Creating backup protects against accidental deletion, malware, ransomware, disasters and hardware failure.
Methods: external drives, NAS, tapes, cloud services.

Data backup strategies

Incremental Backup	Only new or modified data is backed up, saving time and disk space. Ensures you always have the latest version of your data.
Full Backup	Copies all data and allows restoring different versions as needed.to the backup location. Can quickly consume storage if old backups aren’t deleted.

Cloud provider for data Backups

Check IT policy before storing company data.
Considerations: regulations, data ownership, service agreements.
Best practices: strong passwords, limit access, encrypt before upload, monitor usage.

DO NOT *use personal Google Drive, Dropbox, iCloud, or personal email for sensitive data. Always use approved secure channels.*

Indicators of Incidents

Traffic from Unkown Network Addresses	Multiple Failed Login Attempts
Increased Network Bandwidth Usage	Suspicious Emails and Phone Calls
Unlocked Secure Areas	Deleted or Altered Files
Unusual Activities During Off-hours	New Users and Devices in the Network

Proper Storage & Sharing

✔ Store on approved encrypted systems (servers, secure cloud, encrypted drives).
✔ Use access control (limit who can view).
✔ Data minimization – keep only what's necessary.
✔ Share via encrypted channels (secure transfer tools, encrypted email).
✔ Never use unencrypted email, personal cloud, or messaging apps.