Not Sure If It's a Cyber Incident? Start Here.

Your First Response Guide — Keep This Handy

Not Sure What to Do or Whether to Report?
Any event that threatens the confidentiality, integrity, or availability of systems may be a cyber incident.
Including:

- Misuse or unauthorized access to systems
- Data theft or accidental disclosure
- Unauthorized changes to data, hardware, or software
- Credential compromise or login anomalies
- Website defacement or compromise
- Denial of service (DoS) attacks
- Malware or suspicious software activity

Unusual system behavior or performance issues

1. Notify Your Emergency Contacts

- IT Lead: Name - Number-
- Cyber Insurance Provider:
  - NYMIR Claims: nymirclaims@wrightinsurance.com | 800-894-9341
  - Breach Response (Initial Breach Consult Included): cyberclaim@gaig.com | 877-209-2009
- NYS DHS Incident Response Assistance: 844-628-2478
- NYS MANDATED REPORTING:
  - NYS DHS: https://www.dhses.ny.gov/cybersecurity-incident-and-ransom-payment-reporting
  - NYS ITS Cyber Command Center: 866-446-9762 | support@soc.ny.gov
- Internal Leadership

2. Isolate the Threat

- Disconnect affected devices from the network
- Do not power off unless instructed
- Avoid using USB or external drives

3. Preserve Evidence

- Do not delete files, logs, or emails
- Document what was noticed, when, and by whom

4. Activate Your Cyber Incident Response Plan

- Follow your municipality's protocols
- If no plan exists, begin drafting one post-incident

5. Communicate Transparently

- Prepare a public statement if needed
- Keep staff and stakeholders informed

Questions? Contact: Elisabeth Dubois | edubois@wrightinsurance.com | 518-949-0127