

Basic cyber hygiene

- Manage your IT and risk.
- Know your systems, where your data is, and who has access.
- Harden your systems – CIS benchmark (<https://www.cisecurity.org/cis-benchmarks/>) is one way.
- Keep your systems updated – patch, keep your anti-virus up to date, and use vendor supported versions.
- Monitor your systems for strange behavior.
- Applications – Open Web Application Security Project (OWASP) and public scan with a tool such as SSL Labs (<https://www.ssllabs.com/ssltest/>).

Adopt a framework

There are many that exist. Texas state agencies use the [Texas Cybersecurity Framework](#) or choose another that works better for you such as NIST CSF, CMMI, or CCSMM.

Get a cybersecurity assessment

An assessment will let you know how you are doing and can be the basis for modernization, investment, and planning.

There are numerous sources that offer assessments and can even be done at no cost. DIR, the Department of Homeland Security (DHS), or various third parties provide assessments as well.

Have an incident response plan

There are many sample plans on the Internet. The plan should be used in conjunction with Business Continuity planning. DIR offers a template in the [Incident Response Team Redbook](#).

Join MS-ISAC

- The Multi-State Information Sharing and Analysis Center (MS-ISAC) offers many services.
- Join the MS-ISAC to gain access to free resource: <https://www.cisecurity.org/ms-isac>.
- Complete the [Nationwide Cybersecurity Review](#) (NCSR) to identify areas to improve.

Join the Texas ISAO

Join the [Texas ISAO](#) to share information regarding cybersecurity threats, best practices, and remediation strategies.

CISA services and resources

- CISA [National Cybersecurity Assessments and Technical Services](#).
- CISA [Cyber Essentials](#).

DIR resources

- DIR [Security Policy and Planning Resources](#).
- DIR [Managed Security Services](#).
- Complete a Managed Security Services (MSS) Inter Local/Agency Contract through DIR. This is a no-cost option that keeps MSS on retainer and at the ready if needed.

Fraud resource

- Cybercrime Support Network: <https://fraudsupport.org/>
- Data Breach and Credit Monitoring Services: <http://www.txsmartbuy.com/contracts/view/2192>

Train

- <https://www.preparingtexas.org/TrainingCatalog.aspx> (keyword "Cyber")
- [National Cybersecurity Preparedness Consortium](#)
- Federal Virtual Training Environment (free for SLTT): <https://fedvte.usalearning.gov>

Work with your designated emergency management personnel to optimize resources and minimize the impact of an incident.



If You Need Assistance

Contact your Emergency Management Coordinator or Texas Division of Emergency Management (TDEM) District Coordinator <https://www.tdem.texas.gov/regions> or, contact DIR Office of the CISO at 1-877-DIR-CISO (1-877-347-2476) or by email at DIRSecurity@dir.texas.gov.