Cybersecurity in the Midst of Crisis

Ensure your most valuable business data do not succumb to COVID-19

For Everyone

- Maintain Physical Security
  - Follow all office security policies
  - Dispose of sensitive data securely
- Ensure a Secure Connection
  - Avoid public Wi-Fi
  - Set up Multi-Factor Authentication (MFA)
  - Use encrypted communications
  - Set up firewalls
  - Use a secure VPN
- Install Updates & Patches
  - Install updates and patches regularly
- Beware Social Engineering Scams
  - Beware spear phishing attacks, other social engineering scams
- Back Up Data
- Keep Separate Work Devices

For Managers

- Establish a WFH Policy
- Invest in Staff Cybersecurity Training
- Secure Remote Access Systems
  - Test increased capacity
  - Limit privileges
  - Use protective DNS
- Leverage IT Expertise
  - Ensure IT staff can perform remote cybersecurity
  - Increase awareness of IT support for remote workers

Build Resilience

- Know System's Recovery Baseline
- Review Disaster Recovery Procedures
- Update Incident Response Plans for Distributed Workforce
- Report Incidents to DHS CISA