MIIA
CYBER RISK MANAGEMENT

CYBER RISK MANAGEMENT

BEST PRACTICES FOR CYBER SECURITY

1 IDENTIFY OUR KEY ASSETS
- What do we use?
- What is vital to operations?
- Who manages the asset?

2 BACKUP OUR ASSETS
- Resilience to disasters
- Testing the backups
- Physically distribute

3 CONTROL ACCESS CAREFULLY
- Minimize permissions
- Multi-person approvals
- Audit access logs

4 USE STRONG PROOF OF IDENTITY
- Multiple authentication
- Hardware tokens
- Biometrics

5 ENGAGE THE TEAM
- Employees
- Contractors
- Vendors

6 CREATE A RECOVERY PLAN
- Insure assets/recovery
- Know reporting laws
- Ensure mission continuity

7 QUESTION ONLINE INTERACTIONS
- Email may be phishing
- Links may invite malware
- Social engineering is common

8 USE TRUSTWORTHY NETWORKS
- Use VPNs when possible
- Only use secured WiFi networks
- Attacks possible via unknown WiFi

9 USE A FIREWALL
- Corporate firewalls at work
- Software firewalls at home
- Experts can help tune firewalls

10 EDUCATE YOURSELF
- IT trainings about latest threats
- Ask questions about risks
- Learn and follow best practices

Cyber security best practices compiled by Dr. Craig Shue, Worcester Polytechnic Institute for MIIA, January 2020.

For more information on Cyber Security practices – there is a wealth of in-depth information available for members on the MIIA website. Visit eMIIA.org

CONTACT YOUR MIIA ACCOUNT EXECUTIVE FOR MORE INFORMATION.
ONE WINTHROP SQUARE, BOSTON, MA 02110 **800.882.1498**

MIIA A MEMBERSHIP SERVICE OF THE MASSACHUSETTS MUNICIPAL ASSOCIATION