Cyber Risk Management Resources

We want to provide many resources and guides on many of the requirements in the NJ Cyber JIF Cybersecurity Framework, but your technology expert should be your first resource. You will find most the resources we highlight below are governmental entities, most notably MS-ISAC, US-CERT, CIS, NJCCIC and NIST. These organizations provide an extensive array of free resources to public entities, so we encourage contacting them for services.

MEL Cyber Webpage
https://njmel.org/wp-content/uploads/2019/06/Cyber-News_Free-Member-Resources.rev_.pdf

Center for Internet Security (CIS) Guides

- Self-Assessment Tool: https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat
- Enterprise and Software Assets Guide: https://www.cisecurity.org/insights/white-papers/guide-to-enterprise-assets-and-software
- CIS Controls Mapping: https://www.cisecurity.org/controls/cis-controls-navigator/
- Security Services: https://www.cisecurity.org/services

Backups
NJCCIC offers tips for data back-up setups: https://cyber.nj.gov/mitigation-guides/backups-the-cure-to-viral-cyber-infections.

Training
Consider using an outside vendor to provide the training. See the Cyber JIF's Cyber Hygiene Training Vendor guide attached. Cybersecurity Ventures, along with many other organizations, publishes an annual report of top vendors: https://cybersecurityventures.com/security-awareness-training-companies/.

Passwords
Review NJCCIC's and NIST's password recommendations. NIST is the go-to source for cybersecurity standards and NJCCIC typically follows and provides some additional commentary:
https://cyber.nj.gov/instructional-guides/passwords-passwords-passwords
https://pages.nist.gov/800-63-3/

There are many services available to run your organization's email addresses against known breaches, which are typically provided by your security software/SaaS provider, such as Norton, BitDefender, etc. A very popular provider is "Have I Been Pwned?": https://haveibeenpwned.com/.

Multi-Factor Authentication (MFA)
NJCCIC offers an easy technical guide to deploying multi-factor authentication in your organization: https://cyber.nj.gov/instructional-guides/stop-what-you-are-doing-and-enable-mfa.

Government Cyber Memberships
NJCCIC: https://cyber.nj.gov/members/
MS-ISAC: https://learn.cisecurity.org/ms-isac-registration
Water-ISAC: https://www.waterisac.org/
E-ISAC: https://www.eisac.com/
US-CERT / CISA: https://us-cert.cisa.gov/
ICS-CERT: https://us-cert.cisa.gov/ics
IT-ISAC: https://www.it-isac.org/
Elections-ISAC: https://www.cisecurity.org/ei-isac/
Surface Transportation-ISAC: http://www.surfacetransportationisac.org/

Remote Access

This NJCCIC guide offers security tips for remote access: https://cyber.nj.gov/this-is-security/tips-for-teleworkers-remote-access-security.

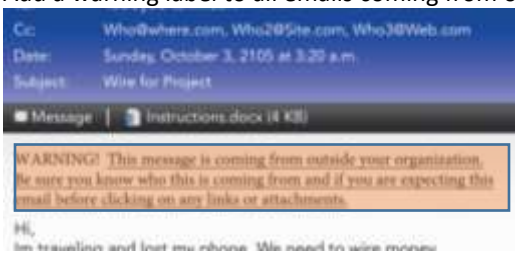
NJCCIC Router security: https://www.cyber.nj.gov/instructional-guides/how-to-configure-and-secure-a-home-wi-fi-router

Banking Controls

See NJ DCA's electronic payroll guide for assistance in this area of banking controls:
https://www.state.nj.us/dca/divisions/dlgs/resources/pdf/payroll%20_agency_%20handbook.pdf

Email Warning Label for Outside Senders

Add a warning label to all emails coming from outside of your organization via the transport server.



Segmentation

NJCCIC guide to Network Segmentation: https://www.cyber.nj.gov/this-is-security/network-segmentation

Employee Policies

Remote Working: AXA XL's partner InformationShield has provided a template Remote Working policy to use with your employees. See attached.

Mobile Device Access & Waiver: AXA XL's partner NetDiligence has provided a template policy for your employee's use of personal devices for work, giving authorization for you to access and wipe the device.