LEADERSHIP AND MANAGEMENT

- There is a clear chain of command regarding notification of possible cyber events and decision-making capabilities, with a command-like operations structure.
- Regular cyber risk management discussions occur among the leadership team.
- Development and implementation of a cybersecurity program that leverages industry standards and best practices (inspired by NIST/NICE).
- Regular evaluation of cybersecurity budgets, plans, partners, incident reports and top-level policies.

ADMINISTRATIVE MAINTENANCE

- There is a quarterly review to ensure correct permissions are granted to each employee, such as access to Personally Identifiable Information (PII) and Sensitive Personal Information (SPI).
- Maintenance of inactive user accounts is delegated to a staff member and routinely overseen by their manager.
- There is a documented Incident Response Plan to deal with threats, including malware detection and treatment.
- System logs are routinely reviewed as directed and stored.
- Cybersecurity and privacy policies, procedures, and plans are reviewed and updated as needed on a quarterly basis.
- An individual or individuals are responsible for reviewing and addressing security news bulletins to maintain security awareness.
- Repeated testing of networks and technology investments via red team activities or third-party pen testing scheduled to accurately assess and remediate vulnerabilities before problems occur.

TRAINING AND EDUCATION

- Biannual discussions with cyber teams about desired skills development needs and growth opportunities.
- Cyber professionals have access to simulated network environments that allow them to practice defending and fighting attacks in real-time.
- Perform mock cyber incident drills with senior executives, staff and cyber professionals to evaluate current security posture.
- Cyber staff receive quarterly assessments to determine skills gap and additional training needed.

NETWORK CONFIGURATION AND TECHNOLOGY

- Systems undergo automatic updates; those delayed are flagged to appropriate IT personnel.
- Ensure continuous monitoring and auditing throughout the system’s full lifecycle.
- Network prevents unauthorized devices from connecting (i.e. USB, flash media).
- Secure web servers and workstations to avoid exploits.
- All systems maintain a current license of an enterprise-grade cybersecurity detection and remediation solution.

EMPLOYEE ALIGNMENT

- Train staff to be ever-ready: be alert, know appropriate actions, understand tools and their use.
- A clearly stated, appropriate password policy is acknowledged by employees and there is a system (technological or otherwise) that confirms protections are properly applied and implemented.
- Full-time employees and contractors receive recurring, mandatory enterprise security training.
- Staff have access to only authorized web browsing.

WE HOPE THIS HELPS YOU GET A MORE HOLISTIC PICTURE OF YOUR CYBER TEAM AND INFOSEC PROCESS. NOW, LET’S CONNECT, SO WE CAN HELP YOU SUSTAIN AND GROW YOUR CURRENT EFFORTS.