MiSecure

Cybersecurity Maturity Grid

Solution	Level 2: Basic	Level 3: Advanced	Level 4: Excelling
Multi-Factor Authentication	Require Multi-Factor Authentication (MFA) on some systems for some staff.	Require MFA on all externally accessible systems, including email and remote access (e.g. VPN, RDP) for all staff.	Require MFA for all accounts, for all staff where possible. Require MFA for administrative account use and other critical internal systems
Training	Provide staff with occasional training and tips to spot phishing emails.	Regularly provide staff with training on cybersecurity best practices including staying vigilant for phishing emails.	Schedule regular skills training and testing using fake phishing campaigns. Provide training and methods to report suspected phishing email
Patching	Perform updates arbitrarily and manually when necessary or noticed.	Perform updates regularly on all systems. Systems that aren't able to be upgraded (e.g. vendor servers) are isolated.	Apply updates to all systems and patch critical vulnerabilities as soon as possible and automatically where possible.
Vulnerability Scanning	Review firewall rules regularly to look for external vulnerabilities.	Set up regular, external vulnerability monitoring to automatically alert on exposed, vulnerable services.	Set up regular, internal vulnerability monitoring and address vulnerabilities immediately.
Passwords	Adopt a password policy requiring strong, complex passwords and change default passwords on all new equipment and devices.	Adopt a password policy that addresses password reuse and expiration. Establish an onboarding process for new equipment and devices that require default password changes.	Enforce industry-standard password policies. Actively search for equipment with default passwords
Backups	Maintain regular backups of all critical technology infrastructure (e.g. servers, switches, routers).	Schedule backups offsite and ensure they are offline and/or immutable.	Test backups regularly and ensure a quick restoration process is documented and tested.
IRP	Discuss within IT what might happen during a cybersecurity incident and adopt a one page Incident Response Plan (IRP).	Adopt a thorough IRP and discuss with both IT and non-IT staff.	Adopt an IRP that is customized for your organization and review it with all involved. Conduct tabletop exercises at least annually.
MDR	Monitor systems for viruses and other indicators of compromise (IOCs).	Monitor all critical technology infrastructure full-time for IOCs with mitigation being conducted 24x7 quickly, and automatically.	Implement protections typically provided by a Managed Security Service Provider (MSSP), including: all district devices are monitored; log files are centrally maintained and monitored; and suspicious account activity is being monitored and addressed.
Assessment	Conduct a cybersecurity assessment using the MiSecure Quick Self Assessment or more sophisticated tools at least annually.	Conduct a cybersecurity assessment using a comprehensive tool such as the CIS CSAT or with a third party. Based on results, establish and address remediation priorities with staff.	Conduct a third party penetration test regularly in order to identify and address weaknesses.
Email Security	Enforce strong email tenant settings.	Implement a phishing monitoring and remediation solution.	Automate the detection and remediation of compromised email accounts.