TECHHEADS

Your Cybersecurity Task Force.

Now, there's a whole new way to deliver ongoing cyber protection. We've done the research, selected the tools, and created the processes you need to diminish vulnerabilities and reduce risk.

Our solutions are informed by the NIST (National Institute of Standards and Technology) Cybersecurity Framework and the Basic CIS (Center for Internet Security) Controls, both of which define best practices for protection. **Your defense plan starts right here.**

ARMOR™ is a critical first step in the cybersecurity battle.

Eliminate potential cracks that hackers can exploit.

Ensure the utmost reliability and security.

- Maintain
- Automate
- Monitor
- Secure
- Train

SHIELD™ protects what is most valuable to your business.

Execute the practices recommended by NIST to strengthen your security posture.

Protect the information, systems and networks that support your business.

- Identify
- Protect
- Detect
- Respond
- Recover

ONBOARD AND GO.

Have your security program up and running in 30-90 days.

Onboarding
Ongoing

Gather. Define. Initiate.

Monitor. Scan. Alert. Log. Assess.

NIST SMB Cybersecurity Fundamentals

ARMOR™ + SHIELD™ are designed to work together to help your organization meet the full set of practices recommended by NIST for small and mid-sized businesses. Review NISTIR 7621 recommendations below:

		ARMOR	SHIELD
2.2	Identify info, stored + used	○	✓
	Determine value of info	○	✓
	Develop inventory, hard + software	✓	○
	Understand threats + vulnerabilities	✓	○
3.1	Identify + control access to business info	○	✓
	Conduct Background Checks	○	○
	Require user accounts for each employee	✓	○
	Create infosec policies + procedures	○	✓
3.2	Limit employee access to data	○	✓
	Install Surge Protectors + UPS	○	○
	PatchOS and apps	✓	○
	Install and activate firewalls on all networks	○	✓
	Secure wireless access point + networks	○	✓
	Setup web + email filters	○	✓
	Use encryption for sensitive business info	○	○
	Complete Full disk encryption	○	✓
	Mobile Device Management	○	✓
	Key/password vault/escrow	✓	○
	Dispose of old computers + media safely	○	○
	Train your employees	✓	○
3.3	Install + update malware programs	✓	○
	Maintain + monitor logs	○	✓
3.4	Develop plan for disasters + infosec incidents	○	✓
3.5	Ensure proper backups	○	✓
	Secure Cyber Insurance	○	○
	Improve processes / procedures / tech	○	✓
4.0	Pay attention to the people around you	✓	○
	Be careful of email attachments + web links	✓	○
	Separate personal + business devices + accounts	✓	○
	Do not connect personal or untrusted hardware	✓	○
	Be careful downloading software	✓	○
	Do not give out personal or business info	✓	○
	Never give out username or password	✓	○
	Watch for harmful pop-ups	✓	○
	Use strong passwords	✓	○
	Change default passwords	✓	○
	Conduct online business more securely	✓	○

Let's get to work.

- Gain key insights to critical aspects of your network
- Identify sensitive data
- Define appropriate access controls
- Create maintenance plans
- Initiate protection and monitoring policies
- Vulnerability assessments
- vCIO strategy sessions
- Daily scans, alerts + logs
- Monthly maintenance
- Quarterly updates
- Bi-annual deep dive
- Annual security assessment

To begin your defense plan with us, visit techheads.com or call (503) 639-8542.