RAMTech

We Make IT Simple.

NIST CYBERSECURITY CHECKLIST

IDENTIFY - Know what you have and what needs protection

- □ We have a list of all computers, laptops, servers, and mobile devices
- □ We know where our business data lives (email, cloud apps, file storage)
- □ We understand which systems are critical to daily operations
- □ We know who has access to what systems and data
- □ We've identified basic cybersecurity risks to the business

PROTECT - Protect your technology, data, and people

- □ Strong passwords are required (no shared passwords)
- □ Multi-factor authentication (MFA) is enabled where available
- □ Employees receive basic cybersecurity awareness training
- □ Business email is secured against phishing and spam
- □ Computers and servers are kept up to date with security patches
- □ Antivirus / endpoint protection is installed on all devices
- □ Data is backed up regularly

DETECT - Know when something isn't right

- □ We receive alerts for suspicious activity
- □ Systems are monitored for unusual behavior
- □ Employees know how to report suspicious emails or activity
- □ Failed login attempts are logged and reviewed
- □ We can tell when a device has not checked in or updated

RESPOND - Act quickly when an issue occurs

- □ We have a basic incident response plan
- □ We know who to call if there is a security issue
- □ We can isolate affected systems if needed
- □ Employees know what to do during a cybersecurity incident
- □ We document incidents and actions taken

RECOVER - Get back to business safely

- □ Backups are tested and can be restored
- □ We can recover systems after an incident
- □ We review what happened and improve defenses
- □ Policies and protections are updated after incidents
- □ Business operations can resume with minimal disruption