CYBERSECURITY FOR
SMALL BUSINESS

Understanding
THE NIST CYBERSECURITY FRAMEWORK

You may have heard about the NIST Cybersecurity Framework, but what exactly is it?

And does it apply to you?

NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection.

You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover.

1. IDENTIFY

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:
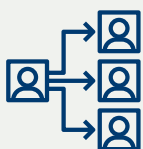
Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.

Steps to take to protect against an attack and limit the damage if one occurs.

2. PROTECT

- Control who logs on to your network and uses your computers and other devices.

- Use security software to protect data.

- Encrypt sensitive data, at rest and in transit.

- Conduct regular backups of data.

- Update security software regularly, automating those updates if possible.

- Have formal policies for safely disposing of electronic files and old devices.

- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

Homeland Security

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SBA
U.S. Small Business Administration

3. DETECT ———

Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.

Check your network for unauthorized users or connections.

Investigate any unusual activities on your network or by your staff.

4. RESPOND ———

Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.

- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

Test your plan regularly.

5. RECOVER —

After an attack:
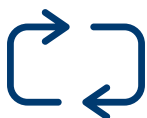
Repair and restore the equipment and parts of your network that were affected.

Keep employees and customers informed of your response and recovery activities.

For more information on the NIST Cybersecurity Framework and resources for small businesses, go to NIST.gov/CyberFramework and NIST.gov/itl/smallbusinesscyber.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

Homeland Security

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SBA
U.S. Small Business Administration