

## First steps to better secure your organization



While cybersecurity can be overwhelming, several simple but effective steps can immediately improve your organization's security posture.


- Implement multifactor authentication (MFA) and a strong password policy
- Invest in cyber liability insurance to protect your business
- Educate your team with security awareness training
- Create an incident response plan [\[download template\]](#)
- Schedule regular vulnerability scans and security assessments
- Encrypt emails and all data both stored and in motion
- Secure your endpoints (especially with BYOD or remote workers)
- Replace legacy products to improve cybersecurity and productivity
- Pay attention to wireless security (guest password updates, anyone?)
- Get serious about access control (physical and digital)
- Craft a business continuity plan with redundancy
- Protect your perimeter with effective firewalls



**Exigent's Security Solutions**

## Don't Overlook Essential Cybersecurity Policies

Implementing clear, comprehensive policies can strengthen cybersecurity, especially when paired with the right tech solutions.

<p><b>Acceptable Use Policy (AUP)</b>                  Defines acceptable and prohibited uses of technology resources such as company computers, emails, and the internet. Clarifies expectations regarding downloading software, sharing information, and online communication.</p>	<p><b>Data Management</b>                  Categorizes data based on sensitivity (e.g., confidential, proprietary, public) and outlines handling procedures for each category. Specifies access controls, storage requirements, and retention periods for distinct types of data.</p>	<p><b>Access Control Policy</b>                  Defines who has access to sensitive data and systems, based on the principle of least privilege. Outlines the process for requesting and granting access and establishes review procedures to ensure continued appropriateness.</p>
<p><b>Password Management</b>                  Establishes minimum password complexity requirements (length, character types, etc.) and update frequency. Prohibits the use of weak passwords and common phrases and encourages the use of password managers.</p>		<p><b>Remote Access Policy</b>                  Defines the rules and procedures for accessing company resources remotely, including approved devices, VPN or SASE usage, and data security practices.</p>
<p><b>Incident Response Policy</b>                  Outlines the steps to take in case of a data breach or security incident, including notification procedures, containment measures, and remediation actions. Ensures a coordinated and effective response to minimize damage and restore operations quickly.</p>	<p><b>Business Continuity</b>                  Define procedures for maintaining business operations and data availability in the event of natural disasters, power outages, or other disruptions. Identify critical systems and data, designate backup locations, and outline recovery processes.</p>	<p>Regularly reviewing and updating these policies, coupled with comprehensive training for all employees, forms the foundation for a strong security culture within your organization.</p>



2 out of 3 small to midsize businesses will have a breach of some sort in the next 12 months.