Network Security Checklist

Helping You Keep Your Network Safe

Network Security Checklist

Many small and medium-sized businesses do not have adequate network security. Here's how to make sure you do.

Network Security Checklist

Every business should have a thoughtfully prepared network security plan. A thorough policy will cover topics such as:

- Acceptable use policy, to specify what types of network activities are allowed and which ones are prohibited
- E-mail and communications activities, to help minimise problems from e-mails and attachments
- Antivirus policy, to help protect the network against threats like viruses, worms, and Trojan horses
- Identity policy, to help safeguard the network from unauthorised users
- Password policy, to help employees select strong passwords and protect them
- Encryption policy, to provide guidance on using encryption technology to protect network data
- Remote access policy, to help employees safely access the network when working outside the office

Answering the following questions can help you develop your own policy:

Do you have any of the following?

- **Firewall**, to keep unauthorised users off your network
- **Virtual private network (VPN)**, to give employees, customers, and partners secure access to your network
- **Intrusion prevention**, to detect and stop threats before they harm your network

For additional SMB security information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

- **Content security**, to protect your network from viruses, spam, spyware, and other attacks
- **Secure wireless network**, to provide safe network access to visitors and employees on the go
- **Identity management**, to give you control over who and what can access the network
- **Compliance validation**, to make sure that any device accessing the network meets your security requirements

Identify Your Most Important Digital Assets and Who Uses Them

- Exactly what are your company's digital assets (such as intellectual property and customer records)?
- What are they worth?
- Where do those assets reside?
- Who has access to these assets, and why? Can all employees access the same assets?
- Do you extend access to business partners and customers?
- How do you control that access?

What Would a Security Breach Do to Your Business?

- What is the potential financial impact of a network outage due to a security breach?
- Could a security breach disrupt your supply chain?
- What would happen if your Website went down?
- Do you have e-commerce features on your site? How long could the site be down before you lost money?
- Are you insured against Internet attacks, or against the misuse of your customers' data? Is this insurance adequate?
- Do you have backup and recovery capabilities to restore information if necessary after a security breach?

Consider Your Current and Future Needs

- How do you expect your business plan to evolve over the next few years?
- How recently have you updated your network equipment? Software? Virus definitions?
- What type of security training do you provide to your employees?
- How will growth affect your digital assets and their value to your business as a whole?
- In the future, are you likely to have a greater need for remote employees, customers, or partners to access those digital assets?

Cisco's Next Gen Intrusion Prevention Systems (NGIPS) are a necessity for a SMB Network to ensure your business network is safe