The Digital Guide's Fact Sheet

Your Cyber security Policy

Here's some things to consider:

- What are the tech assets you need to protect?
    - List your laptops, tablets, phones, smart speakers as well as any other devices or equipment that need consideration. Don't forget your IOT devices at home or the office.
- Identify the potential threats to your devices and your business:
    - Things like phishing, malware, etc. but also anything that may be specific to your business.
- Identify what information is allowed for your team to share online and what IP needs to stay in house.
    - What is the acceptable use of business supplied devices?
    - Do they need a VPN or firewall at home if they will be operating remotely?
    - Are there any sites or applications that should not be run?
- How do you want the business to handle and store sensitive information?
    - client details
    - supplier information
    - price lists
    - passwords.
- Set your requirements around passwords:
    - Will you use a password management system? If so, which one?
    - What's your password protocol?
    - How often do you update passwords?
    - How are they stored?
    - What happens when a team member leaves?
- Explain the importance of unique passwords for each site and application.
- What are your email security requirements?
    - zero-trust policy
    - how to block spam and report suspicious emails
    - when should team members be sharing work emails?
    - opening or clicking on links
    - downloading email attachments.
- How do you handle data?
    - How to identify sensitive data?
    - When can your team share information or data?
    - Where and how do you store any physical files/paperwork?
    - Understanding client privacy.
    - Destroying data securely.
    - Respecting client opt in/out of emails and any GDPR protocols.
- Social media and internet access:
    - What sites are appropriate for viewing/accessing during work hours?
    - What information should be shared online?
    - What sites should team members use their work email to log in with?
- Dealing with your technology:
    - How do you store devices when they aren't in use?
    - Setting sleep times on desktops/laptops.
    - Making sure screens are off when people aren't at their desks.
    - Reporting theft.
    - Running updates/security patches – who is responsible and when is this done?
    - Maintaining antivirus software.
    - Scanning USBs and other portable devices for viruses.
- If a cybersecurity incident occurs:
    - How do the team report any incidents?
    - Do these need to be reported/documented to industry standards?
    - What actions need to be taken internally?
    - How to notify clients if a breach occurs?
    - Roles and responsibilities in event of an attack?

TRACY SHEEN
THE DIGITAL GUIDE