Calder IT Ltd
SUPPORTING BUSINESSES THROUGH THEIR IT JOURNEY

IT Security Checklist

Welcome to Your IT Security Checklist

You've got this checklist because you care about keeping your business safe from cyber threats. It's a smart move. This isn't just a list; it's a practical set of steps that will help you lock down your systems and keep the bad guys out.

Think of this as your IT health check. It's about making sure you've got the basics covered and that you're staying ahead of the risks.

We've kept it clear and to the point, so you can tick off each item and know you're doing your bit to protect your business.

To use this assessment, check the box next to every statement that applies to your organisation.

Password Policies:

Objective: *To ensure that unauthorised individuals cannot easily gain access to systems or data.*

- [ ] **Strong Password Requirements:** Passwords should be a mix of uppercase letters, lowercase letters, numbers, and special characters. The longer the password, the better, ideally, at least 12 characters.

- [ ] **Password Expiry:** Regularly changing passwords can prevent unauthorised access, especially if a password has been unknowingly compromised.

- [ ] **Two-Factor Authentication (2FA):** Encourage or mandate the use of 2FA where available. This adds an additional layer of security by requiring a second form of identification beyond just a password.

- [ ] **Password Storage:** Ensure that passwords are stored securely, to prevent them from being easily deciphered if accessed.

Software Updates:

Objective: *To protect systems from known vulnerabilities that could be exploited by malicious actors.*

- [ ] **Patch Management:** Regularly check for and apply patches to operating systems and applications. Patches often address security vulnerabilities.

- [ ] **Automated Updates:** Where possible, enable automated updates to ensure timely application of critical patches.

- [ ] **Vulnerability Scanning:** Use tools to scan for vulnerabilities that might arise from outdated software.

Backup and Recovery:

Objective: *To ensure data integrity and availability in case of unexpected events.*

- [ ] **Regular Backups:** Schedule daily or weekly backups of critical data. The frequency depends on the volume of data changes and business needs.

- [ ] **Offsite Storage:** Store backup copies in a different location from the original data to protect against physical threats like fires or floods.

- [ ] **Backup Encryption:** Encrypt backups to protect data from unauthorised access.

- [ ] **Recovery Drills:** Periodically test backup recovery processes to ensure data can be restored quickly and accurately.

User Access Controls:

Objective: *To ensure that only authorised individuals can access specific resources.*

- [ ] **Role-Based Access:** Assign access based on roles within the organisation. For example, an HR employee might need access to personnel records but not financial data.
- [ ] **Regular Audits:** Periodically review who has access to what and adjust as necessary, especially when employees change roles or leave the company.
- [ ] **Deactivate Unused Accounts:** Regularly check for and deactivate accounts that are no longer in use, such as those of former employees.

Firewall and Antivirus:

Objective: *To protect systems from malicious threats.*

- [ ] **Active Firewalls:** Ensure firewalls are enabled on all devices, especially servers. Regularly update and review firewall rules.
- [ ] **Regular Scans:** Schedule regular antivirus scans on all systems to detect and remove malware.
- [ ] **Update Virus Definitions:** Ensure that the antivirus software's virus definitions are updated regularly to detect the latest threats.
- [ ] **Intrusion Detection Systems (IDS):** Consider implementing an IDS to monitor network traffic and detect suspicious activities.

Employee Training:

Objective: To ensure that all employees are aware of and can act on potential security threats.

- [ ] **Regular Training Sessions:** Conduct training sessions on security best practices, such as recognising phishing attempts and safely handling data.

- [ ] **Simulated Attacks:** Periodically test employees with simulated phishing emails or other fake threats to gauge their awareness and response.

- [ ] **Clear Reporting Procedures:** Ensure employees know whom to contact if they suspect a security breach or if they receive suspicious communications.

Congratulations!
You're on Your Way to Stronger IT Security

Nice work getting through this checklist. It's a solid start to making your business's IT security tighter. But remember, security isn't a one-time deal. It's an ongoing process, and this checklist is a tool to help you keep on top of it.

Keep this checklist handy. Use it to regularly check up on your IT health. Update it when you need to. And if you ever feel stuck or need more help, remember that there are people out there who can give you a hand.

Your business is worth protecting. So, keep this checklist close, and you'll be doing just that.