Cyber Security Checklist

Assess your cyber security measures with our simple checklist

REMEMBER

We are always here to help if you need us. We are just a phone call or an email away.

Cyber Security is an ongoing project with no simple shortcuts. Do you have the ability to avoid a security breach? This checklist takes you through 10 key questions to help you take a proactive approach to cyber security.

Cyber security also goes hand-in-hand with GDPR as it concerns the protection of personal data from loss, theft, or any kind of unauthorised access. (You may also find it useful to download our GDPR checklist).

Print off the grid part of this document (Page 2-3) and work through it to find out if your organisation completes these tasks. If concerns are raised on any of the fields, you should do all that is reasonably practicable to sort out the issue as soon as possible.

Disclaimer *- this checklist is not a definitive list and Cyber Security responsibilities/duties vary depending on the type and size of businesses. This checklist is to be used as rough guidance only. iHASCO assumes no responsibility for errors or omissions in the contents of this document.*

Cyber Security Checklist

Assess your cyber security measures with our simple checklist

Task	Status	Completion Date
Do you regularly review your cyber security policies and procedures? If not, set a date at least every 6 months to ensure that they're still effective and up-to-date.		
Have you reviewed your data backup procedures and retention/deletion procedures?		
Do you have network & internet security measures in place? (e.g. VPN, firewalls)		
Have you checked that email security is in place and that staff understand how to recognise suspicious emails?		
Do you train staff on the importance of data protection and confidentiality? (e.g. encourage the use of strong passwords)		
Are there procedures in place for ensuring that software updates are installed?		
Are there systems and procedures in place for protecting data accessed by staff using electronic devices - particularly if working remotely?		
Is a plan in place for dealing with any security breaches? Are staff aware of their responsibilities? Is there a business continuity plan?		

Task	Status	Completion Date
Have employees read your cyber security policy?		
Have employees had relevant cyber security training?		

Comments:

For Employers/Responsible Person

1. Do you regularly review your cyber security policies and procedures? If not, set a date at least every 6 months to ensure that they're still effective and up-to-date.

Cyber security threats can have disastrous consequences for your business, you customers/clients, your staff, and for you. It's vital that you regularly look for any vulnerabilities in your systems to ensure that you're protected and your cyber security measures are effective.

2. Have you reviewed your data backup procedures and retention/ deletion procedures?

A business needs a backup strategy to recover lost data and to be able to restore it in an emergency. In fact, backup and disaster recovery is part of the GDPR. It requires you to be able to restore personal data in the event of a physical or technical incident as well as test any recovery procedures to ensure they are effective and can be completed in a timely manner.

3. Do you have network & internet security measures in place? (e.g. VPN, firewalls)

It's important to use measures such as VPN, firewalls and anti-malware software applications, for example, to secure your network. Check that your hardware devices provide you with the required security and continue to monitor the effectiveness of them.

4. Have you checked that email security is in place and that staff understand how to recognise suspicious emails?

Emails are particularly vulnerable to cyber breaches. Review your email security and check systems are in place to prevent threats from all incoming and outgoing emails. An email policy can help staff identify what types of information cannot be put in an email, such as passwords or personal data. The best way to help staff recognise suspicious emails is by providing examples and highlighting any incidences when they have been received.

5. Do you train staff on the importance of data protection and confidentiality? (e.g. encourage the use of strong passwords)

A poor password is a poor defence. You need to make sure that your staff understand this. Help them understand what makes a password good or bad - you can use online password strength checkers to help them and demonstrate how weak passwords can leave your systems vulnerable.

6. Are there procedures in place for ensuring that software updates are installed?

Any software updates should be installed as soon as they are available, as they often also provide updated security features. Some updates are automatic, though some require input from the user. Check your procedures and make sure that your staff are made aware when they need to do something themselves.

7. Are there systems and procedures in place for protecting data accessed by staff using electronic devices - particularly if working remotely?

With remote working being the new norm, it's more important now than ever before to make sure that your ability to keep remote devices secure is up-to-date. Consider how you protect devices from unauthorised access, how you might lock or secure a lost or stolen device, or what kinds of data you allow off your premises and how it's transported.

8. Is a plan in place for dealing with any security breaches? Are staff aware of their responsibilities? Is there a business continuity plan?

Be prepared for a security incident - even the most robust planning can't offer you 100% protection so you must have a plan in place to deal with one if it happens. Do you have a plan for dealing with a breach in a timely manner and do staff understand what they need to do/who they need to alert if it does? A comprehensive plan aims to reduce the impact of the breach and help you get back up to speed as soon as possible.

9. Have employees read your cyber security policy?

It's vital that all employees have read your cyber security policy to ensure that they understand any security measures you've put in place as well as what their

responsibilities are. It should cover both internal and external breaches whether accidental or deliberate.

10. Have employees had relevant cyber security training?

A large percentage of cyber security breaches result from a lack of staff awareness and the only way to deal with this is to ensure that they've been adequately trained to recognise and deal with dangers.

How iHASCO can help you...

Our Cyber Security Awareness training course provides an overview of the types of cyber security threats that can leave your business vulnerable. By educating all staff members it helps provide the knowledge and awareness required to be vigilant and minimise the risk of a cyber attack. It also includes practical advice for keeping information safe as well as what to do if a breach may have occurred, to reduce its impact.