CYBER SECURITY EMERGENCY PLAN

Fill out this plan and refer to if you ever need to respond to a cyber security incident.

This plan will help you keep your important information safe. This will reduce the stress and time spent dealing with a ransomware attack.

Get to know your important information and devices

Know what you are willing to live without and what you will go above and beyond to save.

With your information and devices, you need to consider:

1. What you can and cannot replace
2. What you will invest to recover the information or device.

What is it?	**Impact if it is lost?**	**Where is it?**	**Do you have copies? Where?**
e.g. Customer database	Loss of historic customer transactions and details	Main server	Yes – cloud backup and offline external storage device
Backups – your Plan B			
Where is it?	**How often is it backed up?**	**How often is it tested?**	**Is it disconnected from your device?**
Devices			**Software and apps**
• Mobile phones • Laptops, desktops • Tablets • Printers • EFTPOs machines			• Shopify • Office 365 • Facebook • Squarespace • Wix • MYOB
Type of device?	**Who owns the device?**	**Used daily, weekly, monthly or rarely?**	**Name of sofware applications?**	**Who has access?**
Emergency contacts		**Email accounts**		
• Bank (fraud) • IT company • Internet provider		• Outlook • Gmail • Yahoo!		
Who you need to notify?				
• Manager • Staff • Colleagues • Customers • ReportCyber • Cyber Insurance				
Who	**Contact**	**When to notify**		