

# CYBER SECURITY CHECKLIST FOR SUCCESS

**WICRESOFT**  
Managed IT Services

This checklist ensures a comprehensive evaluation of your cyber security posture. Do you have questions about the checklist? [Contact our team](#) and we will be happy to assist you.

## Security Analysis and Updates

- Security Audit and Review:** Conduct a thorough audit of your current cyber security measures. This should involve assessing all your security protocols, software, hardware, and network infrastructure. Look for any vulnerabilities that might have emerged over the year.
- Update and Patch Systems:** Ensure all your software, especially security software, is up to date with the latest patches. Outdated systems are a common entry point for cyber threats.
- Review User Access Controls:** Audit who has access to what within your organization. Remove unnecessary access privileges, especially for employees who have changed roles or left the company.
- Physical Security Check:** Don't neglect physical security. Ensure that servers, data centers, and other sensitive areas are secure.

## Data Management and Protection

- Data Backup and Recovery Plan Review:** Verify that your data backup systems are working correctly. Test your recovery plan to ensure it's effective in case of a data breach or loss.
- Password Policies and Management:** Enforce strong password policies and consider implementing multi-factor authentication. Also, encourage or mandate regular password changes.

## Policy Development and Compliance

- Review and Update Cyber Security Policies:** Update your cyber security policies to reflect any new threats or business changes. Ensure these policies are well-documented and accessible to relevant personnel.
- Compliance Review:** Ensure that your cyber security practices comply with relevant laws and industry regulations.
- Incident Response Plan Update:** Review and update your incident response plan. Ensure it aligns with current best practices and includes clear protocols for different types of security incidents.
- Employee Training and Awareness:** Reinforce cyber security awareness among your employees. Provide training on new threats, phishing tactics, and safe internet practices. Remember, your employees can be your first line of defense.

## Insurance and Financial Planning

- Cyber Insurance Policy Review:** If you have cyber insurance, review your policy to ensure it covers current risks and reflects the scale of your operations.
- Vendor and Third-Party Assessment:** Review the security measures of your vendors and third-party service providers. Ensure they meet your cyber security standards.
- Invest in New Technologies:** Evaluate and consider investing in new cyber security technologies that could better protect your business.
- Prepare a Cyber Security Budget for the New Year:** Allocate sufficient resources in your budget for cyber security measures, including training, software updates, and potential consultancy costs.

## About Wicresoft

At Wicresoft, we provide top-notch solutions in managed IT services, Microsoft 365 backup, and email security to businesses beyond Cheshire and the greater Manchester area. Trust us for all your technology needs and experience the difference of working with a dedicated IT partner. Get in touch with us today to elevate your business to new heights.