Cyber Security Solutions

Business Continuity: **On-premise and Off-site Backups / Disaster Recovery**	Ensures that your data is always protected and your business will continue regardless of any hardware failure, loss of your entire facility, and/or breach of your network.
Microsoft 365 Business -Includes many of the solutions below	• Office on tablets and phones • Fully installed and web versions of Office apps • 1 TB file storage and sharing • Business class email (50GB), calendar, and contacts • Online meetings (instant messaging, audio, and HD video chat/conferencing) • Microsoft Teams chat-based workspace • Outlook Customer Manager, Bookings, Invoicing, MileIQ • Helps protect your business from unsafe attachments, suspicious links, and other unseen malware through attachment scanning and link checking. • Information Protection Policies to help control & manage how information is accessed. • Controls to protect your company data on personal mobile devices • Preservation, Compliance & Archiving capabilities with continuous data backup that is accessible anytime/anywhere. • Securely manage iOS, Android, Windows, and macOS devices • Self-service PC deployment with Windows AutoPilot • Simplified controls to manage Windows 10 Pro PCs • Get upgraded to Windows 10 Pro from Windows 7, 8 or and 8.1 Pro

Office 365 Backup and Archiving to a Third Party (not Microsoft)	Ensures that all your email will be recoverable in the event that Microsoft loses or corrupts it. Microsoft recommends this in their Terms of Service: https://www.microsoft.com/en-us/servicesagreement/
Password Manager	Secure password management for all users. Provides a variety of reports and Risk Analyses, based users' passwords. Required in many Financial, Healthcare, and Government-related industries.
Anti-Virus	Prevents viruses, spyware and malware on the device. Required in many Financial, Healthcare, and Government-related industries.
Comprehensive Gateway Security Services	Inspects all traffic and blocks viruses, malware, and other threats. Required in many Financial, Healthcare, and Government-related industries.

24/7/365 Monitoring	Monitors your entire network and devices, alerting on any anomaly, outage, failure, and/or potential failure. Also provides, patch management, detailed inventory reports, software distribution, policy management and enforcement, and secure remote access to any device for your support team. Required in many Financial, Healthcare, and Government-related industries.
Advanced Web-based Threat Protection	Disallows access to sites that spread malware and other threats.
Cyber Security Training, Fake Phishing Campaigns, and Dark Web Monitoring	Provides ongoing Cyber Security Education and testing, fake phishing campaigns, and alerting when usernames and passwords are found on the Dark Web. Required in many Financial, Healthcare, and Government-related industries.
Vulnerability Scans	Tests all public IP addresses for the OWASP Top 10 Vulnerabilities, ensuring that there are no vulnerabilities and/or open ports for hackers to infiltrate. Required in many Financial, Healthcare, and Government-related industries.
Encrypted Laptops and Desktops	Protects data stored on those computers. If they are lost or stolen, all the data is encrypted.

Encrypted Email	Allows you to send proprietary information, personally Identifiable Information, Financial Information, and personal Health Information securely. Required in many Financial, Healthcare, and Government-related industries.
Secure Cloud File Sync and Share (includes encrypted email)	Allows you to encrypt and securely share sensitive proprietary information, personally Identifiable Information, Financial Information, and personal Health Information. Required in many Financial, Healthcare, and Government-related industries.
Email Continuity/ Spam Filter	Blocks viruses, spyware, and malware in emails inbound and outbound. Provides access to recent emails, allowing you to send and receive emails if/when your email server/service provider is down.
Two Factor Authentication	Provides additional layer(s) of protection beyond username and password. Required in many Financial, Healthcare, and Government-related industries.

Mobile Device Management	Allows us to configure and enforce Cyber Security policies on mobile devices, thereby protecting them and the data contained on them. Provides secure remote wipe capabilities and other management tasks. Required in many Financial, Healthcare, and Government-related industries.
Data Loss Prevention	Alerts on potential data leaks and allows us to configure company-wide policies to limit potential vulnerabilities, including USB ports, cloud repositories, etc. Required in many Financial, Healthcare, and Government-related industries.
Security Information and Event Management SIEM	This goes beyond monitoring, using Big Data and Artifical Intelligence to learn about your network and individual user behaviour. Alerts on a variety of potential threats.