Cybersecurity Readiness Checklist

Cybersecurity Readiness Checklist for Toronto Businesses

FOUNDATION CONTROLS
[ ] Multi-factor authentication enabled on all accounts (email, cloud, VPN)
[ ] Password manager deployed for all staff
[ ] All default passwords changed on all devices and accounts

NETWORK AND ENDPOINT SECURITY
[ ] Firewall configured and rules reviewed in last 6 months
[ ] Endpoint protection (EDR) on all computers and servers
[ ] Remote access via VPN only - no direct RDP exposed to internet
[ ] Guest Wi-Fi network separated from business network

PATCH MANAGEMENT
[ ] Automated Windows/macOS updates enabled on all devices
[ ] All business software on supported, current versions
[ ] Monthly patch review process documented and assigned

BACKUP AND RECOVERY
[ ] Automated daily backups running for all critical data
[ ] Backups stored offsite or in cloud (not just local drive)
[ ] Backup restore tested successfully in last 90 days
[ ] Recovery time objective (RTO) defined and documented

STAFF AWARENESS
[ ] Phishing simulation run in last 6 months
[ ] Staff know how to report suspicious emails
[ ] Clear process for reporting lost or stolen devices

INCIDENT RESPONSE
[ ] Written incident response plan exists
[ ] IT provider emergency contact saved by all staff
[ ] PIPEDA breach notification obligations understood

Provided by ITBizTek - Managed IT Services Toronto
itbiztek.com | info@itbiztek.com