CONFIDENCE IT

IT STRATEGY CHECKLIST

NEED HELP?

📱 SCAN ME

C-IT.CO.UK

SETUP

□ Make a Floor Plan

Note: Include location of the server room, workstations, network points, printers etc...

□ Choose an Internet Service Provider (ISP)

Name of Supplier__________________________________

□ Choose a Second ISP installed for resilience

Name of 2nd Supplier__________________________________

CABLING & NETWORK PORTS

□ Cable run locations

□ Router location

□ Printer locations

□ Server location

□ Workstation locations

□ Wireless Access Point locations

□ UPS location

Note: Count electrical outlets and network ports available

□ Port locations and port numbers

Note: Count number of ports required at each location.

WHAT TO SET UP FIRST

□ Server Room

□ Network infrastructure

□ Router/s

□ Wireless Access Points

□ UPS

□ Workstations

□ Printers

INFRASTRUCTURE

Purchasing

□ New equipment - is compatible with existing equipment

□ New equipment - is suitable for business use

Note: Avoid using consumer-made products. Use made for business only.

□ Purchase Server, NAS devices, Network Switches, Wireless Access Points & Peripherals

Note: Consider the growth of business when buying servers, switches and storage.

□ Choose an operating system standard

□ New equipment warranties

Installation

□ Installation work by Name of installer________________________________

□ Installation by vendor Name of vendor ________________________________

Note: Document support and service agreement if required.

□ Drivers and firmware updated

□ Equipment is catalogued

Note: Document serial numbers, purchase dates and use asset tags.

□ New servers, workstations and mobile devices are protected by anti-virus

Operations

□ Review your IT infrastructure regularly

Note: Check warranties and either renew or replace equipment.

□ Review new technologies and investigate if they would benefit your business

□ Maintain a list of all service contracts and vendor contract information

□ Monitor performance of servers, routers, wireless access points, workstations and either upgrade or replace before they become an issue

SOFTWARE

- □ Document a whitelist of allowed applications on workstations and mobile devices
- □ Device management software for deploying software, security patches and updates
- □ Update policies in place for your Operating System, anti-virus and applications
- □ Assign administrative privileges to authorised IT team
- □ Apply multi-factor authentication where available
- □ Software to be purchased and installed from trusted sources
- □ Audit, document and maintain a list of software installed on each device with a record of licence keys
- □ Maintain a list of accounts used for online services, stored in an admin only area
- □ Make someone responsible for monitoring and renewing domain names and hosting services
- □ Email SPAM filter in place for all users
- □ Web filtering in place for all users

THE CLOUD

□ Check and review your company data privacy obligations regularly

□ Create and regularly check policies around those obligations

□ Document which of your business services are stored in the cloud

□ Define and document your cloud services providers SLA and that it is consistent with your own business requirements

□ The SLA has clauses for response time, business continuity and disaster recovery

□ Someone in house or from your IT MSP are responsible for maintaining cloud software and updates

Person responsible ______________________________________

□ Cloud data access is restricted to authorised users

□ Make a plan for loss of access to cloud services

□ Make a plan for a data breach on cloud services

CYBERSECURITY

□ Create a password policy to make password strong and secure

□ Limit system access based on job roles and requirements

□ Only use software that was purchased legitimately form a reputable source

□ Advise staff to not use public Wi-Fi or to use a VPN if they do not have another option

□ Have a policy to lock laptops and devices not in use

□ Have a policy for using external storage devices. Lock it down to authorised user and scan devices before use

□ Schedule daily and weekly backups of critical data to various locations both physical and on cloud

□ Create a disaster recovery and business continuity plan

□ Train staff on the disaster recovery process

□ Create an acceptable use policy that covers the use of company workstations, mobile devices and IT resources

□ Create a social media use policy

□ Regularly review and audit data and software access permissions

□ Create disk quota policies to limit employee use of cloud services and servers

□ Train employees how to use the software and hardware for their role

□ Create a plan to isolate any infected device to remove any threats before re-joining to the network

□ Train staff on cybersecurity threats regularly

□ Conduct phishing threat and network penetration tests regularly

□ Create and maintain a company FAQ document on company IT use and security policies

□ Create disk quota policies to limit employee use of cloud services and servers

NOTES