

Antivirus, antimalware and firewall

- Purchase and install antivirus software. Ensure it is configured for regular scans
- Purchase and install antimalware software. Ensure it is configured for regular scans
- Enable software firewalls on enabled on all business devices
- Use a boundary firewall to at each physical premise (unless part of a managed office)

Device and software policies

- Ensure all devices and software are configured with consistent secure default settings
- Change default passwords on new devices (including firewalls)
- Uninstall unnecessary included software
- Disable auto-run features
- Disable any users accounts and services not needed
- Use automatic screen locking to authenticate access to devices
- Set six-digit pins on all mobiles devices as a minimum
- Set 12-character passwords across endpoint devices
- Create a bring-your-own-device (BYOD) device policy (outline password policies, network access and regular software updates)
- OPTIONAL: Implement a mobile device management solution for BYOD devices
- Maintain an inventory of all devices owned by your business and the software installed on them (noting unique ID, who is responsible for them, etc)
- Create an approved list of tools people can use
- Set up an internal software approval process people can use to request tools

User access control

- Determine how access is granted in line with least privilege principle
- Create a user account creation and approval process
- Regularly review and disable inactive accounts
- Perform administrative activities through a separate user account from your day-to-day login that access the internet and email
- Encourage unique passwords and PINs across accounts and users
- Deliver staff awareness training that demonstrates password best practice
- Grant self-service password reset abilities across systems
- Enable multi-factor authentication (MFA) as a default across all online services

Cloud-based data protection

- Employ VPN access or on-premises VDI if using on-premises servers for remote workers (and ensure these are secured by MFA)
- OR
- Migrate data to a cloud-based service
 - Identify and classify sensitive data based on its value and sensitivity level, using tags or metadata

Email filtering

- Use a reliable email client
- Invest in an enterprise-grade email filtering tool

Website blocking

- Set up network-level blocking through firewall configuration, DNS filtering or proxy server configuration (may be available through your existing security tools)
- Set up purchase specific web filtering software to block access or install browser extensions (may be available through your existing security tools)

Data backup and disaster recovery

- Audit the systems and data you have and how critical they are to operations
- Conduct risk assessments that identify possible disaster scenarios and the effort required to recover (identifying your Recovery Time Objective and Recovery Point Objective)
- Use your Recovery Time Objective and Recovery Point Objective to determine backup frequency and retention timeframes
- Schedule regular on-site and off-site backups
- Refine a data retention policy (outline the rules for retaining data and procedures for destroying it)
- Create and document disaster recovery plan (covering systems to be prioritised, data backup, communications, vendor management and employee training)
- Assemble and train your incident response team
- Configure your recovery site (hot, warm or cold)



Alerts and monitoring

- Invest in tools like XDR, SIEM or SOAR to create an internal security operations centre
 - Recruit resource to operate the security operations centre
- OR
- Outsource your security operations centre to an external cyber security partner

Patch management

- Schedule in regular updates across operating systems, applications, firewalls, etc.
- Centralise management of patches to apply updates organisation-wide
- Apply critical security patches within 14 days of release
- Remove, upgrade or segregate unsupported software

User awareness training

- Hold regular user awareness training (covering how to spot suspicious activity, password best practice, using approved applications, data sharing and threat raising)
- Circulate documents outlining best practices

