

Employee IT Onboarding Checklist

Set new staff up securely from day one, with approved accounts, the right access, MFA, a prepared device and security awareness training.



Complete one copy for each new starter. Record who completed each task and when, then file it with the employee's records.

Employee name

Position

Department

Start date

Manager

Completed by

Security reminder

Never write passwords, MFA codes, recovery codes or other secret authentication information on this document or share them with anyone, including IT support. Give new starters temporary passwords through a secure channel and require them to change it at first sign-in.

Before day one

Done	Task	Responsible person	Date completed
☐	Account creation is approved A manager has formally requested the account and confirmed the start date.		
☐	Access permissions are appropriate Access is based on the role, not copied from another user. Only the systems and folders needed are granted.		
☐	Device is prepared The device is updated, has required software and is enrolled in management where used.		
☐	Endpoint security is installed Antivirus or endpoint protection is installed, active and reporting.		
☐	Device encryption is enabled BitLocker or FileVault is on and the recovery key is stored securely by the business.		
☐	Required software is installed Licensed, approved applications only.		
☐	Equipment is allocated Laptop, phone, headset, security key or other equipment is assigned and recorded.		

On day one

Done	Task	Responsible person	Date completed
☐	MFA is set up The employee registers an authenticator app or security key in person or over a verified call.		
☐	Email is configured Mailbox, signature, shared mailboxes and calendar access are working.		
☐	Password manager is set up where approved The employee has access to the business password manager and shared vaults they need.		
☐	Acceptable-use policy is provided The employee has read and acknowledged the company acceptable-use policy.		
☐	Security awareness training is assigned Training on phishing, safe payments and reporting incidents is completed or scheduled.		

After setup

Done	Task	Responsible person	Date completed
☐	Asset register is updated Devices and equipment are recorded against the employee in the IT asset register.		
☐	Manager approval is recorded The manager confirms the employee has the access they need and nothing more.		

Sign-off

Manager name

Manager signature

Date

Notes

Need a hand?

Omnicon I.T. Services can help you put this into practice. Visit omnicon.com.au/contact-us, call **(03) 9022 1376** or email admin@omnicon.com.au.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.