

Employee IT Offboarding Checklist

Remove access safely when someone leaves, while protecting business data, transferring ownership and meeting retention obligations.



Complete one copy for each departure. Work in the order shown: protect access first, transfer ownership second, and only remove anything once retention requirements have been checked.

Employee name

Position

Department

Confirmed departure date and time

Manager

Authorised administrator

Coordinate with your authorised administrator

Carry out these steps only with the employer's authorised administrator, and in line with your legal, employment and record-keeping obligations. **Do not delete the employee's account, mailbox or files** until ownership has been transferred and you have confirmed how long the data must be kept.

Protect access

Done	Task	Responsible person	Date completed
☐	Departure date is confirmed HR or management has confirmed the final date and time access should end.		
☐	Access removal is authorised A manager has approved the access changes in writing.		
☐	Account is disabled Sign-in is blocked at the agreed time. Disabling, rather than deleting, keeps data available.		
☐	Active sessions are revoked where supported Sign-in sessions on phones, browsers and apps are signed out.		
☐	MFA and recovery methods are reviewed The person's MFA methods and recovery phone or email are removed from business accounts.		
☐	Remote access is removed VPN, remote desktop and remote support access is revoked.		
☐	Shared credentials are rotated where required Passwords the person knew for shared accounts, Wi-Fi or systems are changed.		

Done	Task	Responsible person	Date completed
☐	Third-party application access is reviewed Access to cloud apps, supplier portals and social media accounts is removed or transferred.		

Transfer and retain

Done	Task	Responsible person	Date completed
☐	Email and file ownership is transferred Mailbox access, forwarding or conversion to a shared mailbox, and file ownership are handed to the manager or successor.		
☐	Data retention requirements are checked You know how long email and files must be kept for legal, tax or contractual reasons before anything is removed.		
☐	Devices are collected Laptops, phones, security keys, access cards and other equipment are returned.		
☐	Asset register is updated Returned devices are recorded and reassigned, wiped or retired as appropriate.		

Verify

Done	Task	Responsible person	Date completed
☐	Completion is verified A second person confirms that access is removed, data is retained and equipment is accounted for.		

Verified by

Date

Signature

Notes

Need a hand?

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