

Introduction

Effectively managing the offboarding process when employees leave will ensure a smooth transition and help protect your business from potential risks. This fact sheet provides essential steps small businesses should follow when offboarding employees to maintain cyber security, ensure compliance, and protect business interests.

Why is offboarding important?

- **Security Risks:** Prevent unauthorised access to company systems, data, or assets by revoking access promptly.
- **Business Continuity:** Ensure a smooth transition of duties and protect important client and business relationships.
- **Compliance:** Meet legal obligations related to final pay, benefits, and any non-compete clauses

Incomplete offboarding can lead to significant cybersecurity, operational, and legal risks if former employees retain access to systems, sensitive data or business assets after they leave. If a handover isn't completed correctly, key business knowledge or understanding can also be lost.

Key steps for offboarding employees

- ☐ 1. **Notify key departments:** Alert HR and finance to coordinate payroll and outstanding entitlements, as well as IT to plan for when access removal should occur.
- ☐ 2. **Revoke access and change passwords:** Immediately revoke access to company systems, networks, and confidential data. Change passwords to all business accounts the employee had access to, including email, project management tools, and cloud storage.
- ☐ 3. **Recover company assets:** Collect laptops, phones, access cards, and other company property. For devices that are no longer usable, follow proper disposal or recycling protocols
- ☐ 4. **Dispose of devices and accounts:** If devices are being retired, ensure proper data wiping or destruction to prevent sensitive information from being accessed. If the employee had access to cloud accounts or online services, ensure these accounts are closed or transferred to active team members.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Key steps for offboarding employees cont.

- ☐ 5. **Use document shredding services:** Safely dispose of any sensitive printed documents. Consider using professional document shredding services to ensure that no confidential information can be retrieved from discarded paperwork.
- ☐ 6. **Manage knowledge transfer:** Ensure a thorough handover of ongoing projects, client relationships, and critical documentation.
- ☐ 7. **Review non-compete agreements:** If applicable, ensure departing employees understand and comply with any non-compete or confidentiality clauses.
- ☐ 8. **Exit communication:** Clearly communicate the employee's departure internally and to relevant external stakeholders & clients that the employee had ongoing relations with.

Legal and compliance considerations

- ☐ **Data privacy:** Securely remove the departing employee's access to sensitive client, colleague, or business data.
- ☐ **Record-keeping obligations:** Small businesses must keep accurate employee records (onboarding documentation, pay slips, time sheets, leave records) for 7 years, as mandated by the Fair Work Act. It is best practice to archive ex-employee records so that they are not routinely accessible.
- ☐ **Privacy Act:** If your business handles personal information, ensure you comply with the [Privacy Act 1988](#).

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Tools and resources to assist in offboarding

- ☐ **Password Management:** Use [password managers](#) to revoke access to all business accounts and change shared passwords, as necessary.
- ☐ **Cloud backup and data disposal:** Backup all necessary files before offboarding. For devices no longer in use, ensure proper data wiping and disposal protocols to protect sensitive information.
- ☐ **Human Resources software:** HR tools to manage access, payroll, and exit documentation, ensuring compliance with legal obligations.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 170 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.