love your numbers

CHECKLIST

User Access and Offboarding Checklist

A practical access review for accounting, payroll, banking and connected finance systems, and what to do when roles change.

BEFORE YOU START

This is practical access governance for finance systems. It is not specialist cybersecurity advice. Where you need a security assessment, incident response or technical controls beyond user access, engage an appropriate cybersecurity specialist.

Access tends to accumulate

Access is usually granted quickly and removed slowly. Over a few years a small business can end up with former staff, past advisers and unused apps still connected to its accounting and banking systems.

This checklist is a periodic review and an offboarding routine. Work through it once, then set a date to repeat it.

1. Who currently has access

- [ ] List every user in the accounting file.
- [ ] List every user in the payroll system.
- [ ] List everyone with access to business banking.
- [ ] List advisers, contractors and external providers with access.
- [ ] Note anyone on the list you cannot immediately account for.

2. Is the access role-appropriate

- [ ] Does each person have the access their role actually requires?
- [ ] Is anyone holding elevated access from a previous role?
- [ ] Are preparation, approval and payment release separated where practical?

© 2026 Love Your Numbers Pty Ltd. All rights reserved.
You're welcome to use this checklist in your own business. Please don't copy, sell or share it publicly without our permission.

- [ ] Is payroll access limited to those who need it?

3. Multifactor authentication

- [ ] Is multifactor authentication turned on where the system supports it?
- [ ] Is it in place for banking and payment access?
- [ ] Is it tied to a device or method the business can still reach if the person leaves?

4. Administrator and owner accounts

- [ ] Does the business own the administrator account for each system?
- [ ] Is there more than one person who can administer, so access is not lost?
- [ ] Is the subscription or billing owner known?

> WATCH FOR
> Administrator ownership sitting with a departing staff member or a former provider is a common and avoidable problem. Confirm it before it becomes urgent.

5. Shared logins

- [ ] Identify any login used by more than one person.
- [ ] Replace shared logins with individual users where the system allows it.
- [ ] Where a shared login cannot be avoided, document who has it and when it was last changed.

6. Connected apps and integrations

- [ ] List the apps connected to your accounting and payroll systems.
- [ ] Confirm each connection is still in use.
- [ ] Identify who set up and who maintains each one.
- [ ] Disconnect integrations that are no longer needed.

© 2026 Love Your Numbers Pty Ltd. All rights reserved.
You're welcome to use this checklist in your own business. Please don't copy, sell or share it publicly without our permission.

7. Banking and payment access

- [ ] Confirm who can view accounts, who can prepare payments and who can authorise them.
- [ ] Confirm the process for changing authorised users with your bank.
- [ ] Review any saved payment details or templates.

8. When someone leaves or changes role

Decide what triggers an access review: resignation, role change, end of a contract, or the end of an engagement with a provider.

- [ ] Who is notified when someone leaves?
- [ ] Who is responsible for removing access, and by when?
- [ ] Is access removal part of the offboarding routine rather than an afterthought?

9. Removing access and changing credentials

- [ ] Remove the individual user rather than only changing their permissions.
- [ ] Change any shared credentials the person knew.
- [ ] Update banking authorities where the person was authorised.
- [ ] Reassign anything the person owned, including app connections and administrator rights.
- [ ] Confirm the removal was completed rather than requested.

10. Document who owns what

- [ ] Keep a current list of systems, administrators and users.
- [ ] Note who maintains each connection.
- [ ] Store the list somewhere the business controls.

© 2026 Love Your Numbers Pty Ltd. All rights reserved.
You're welcome to use this checklist in your own business. Please don't copy, sell or share it publicly without our permission.

11. Set a review date

Access drifts quietly. A short scheduled review catches far more than an annual clean-up prompted by a problem.

NEXT STEP

Pick a recurring date, put a name against it, and review the user lists then rather than when something goes wrong.

12. When you need a specialist

If you are dealing with a suspected breach, fraud, compromised credentials or a broader security assessment, that is specialist work. Engage a cybersecurity professional rather than treating it as an access tidy-up.

WHAT NEXT?

If the access list raised more questions than answers, a workflow and systems review is usually the practical next step.

- Bookkeeping
- Payroll

Book a free introductory call
www.loveyournumbers.com.au/contact

Love Your Numbers Pty Ltd. General information only. It is not tax, workplace or financial advice, and it does not replace advice from the relevant authority or a suitably qualified adviser for your circumstances.

© 2026 Love Your Numbers Pty Ltd. All rights reserved.
You're welcome to use this checklist in your own business. Please don't copy, sell or share it publicly without our permission.