1(888)-575-7973
info@lighthouseintegrations.com

LIGHTHOUSE
Partnering For Success Through Innovative Technology

Principle of Least Privilege (PoLP) Checklist

Control Who Has Access to What In Your Business.

Disclaimer: This checklist is provided by Lighthouse Integrations for educational and informational purposes only. It is a general guide and should be adapted to meet your organization's specific legal, regulatory, and operational requirements. Lighthouse Integrations assumes no responsibility or liability for its use.

Step 1: Identify What's Most Important

☐ Make a List of Your Critical Systems & Data

You can't protect what you don't know about. In most small and mid-sized businesses, the most critical assets include payroll, accounting software, customer records, HR files, and intellectual property. These are the areas attackers target and where costly mistakes can happen.

Sit down with your leadership team (or just yourself if you're a smaller business) and ask: "If this system or file disappeared tomorrow, would we still be able to run the business?" If the answer is "no," it belongs on your critical list.

Step 2: Define Access Based on Role

☐ Set up access levels by job function (Finance, Sales, HR, etc.).

When access is granted person by person, it becomes inconsistent, messy, and risky. By grouping permissions by role, you make onboarding and offboarding cleaner and avoid the "just give them everything" shortcut.

Write down the different roles in your business. For each role, decide what systems and files they need to do their job. Example: Finance staff get access to accounting and payroll; Sales gets access to the CRM and client files; Marketing gets access to campaigns and content folders.

Step 3: Set "No Access" As The Default

- [ ] **Make zero access the starting point for new accounts.**

It's far easier to add access than to try and remove it later. If someone starts with broad access, they may keep permissions they never needed in the first place. That creates unnecessary risk.

Work with whoever manages your IT. When new accounts are created, whether in Google Workspace, Microsoft 365, or a payroll system, set permissions to none by default. Add access only as required.

Step 4: Seperate Files and Systems

- [ ] **Keep sensitive data (finance, HR, customer info) in separate places with restricted access.**

The fewer people who can see sensitive data, the lower the chance of an accidental leak or intentional misuse. Segmentation also reduces damage if an account is hacked.

In cloud storage (Google Drive, SharePoint, Dropbox), create folders that are restricted to specific roles. In business apps, review settings to ensure access is limited to relevant teams. For example: Marketing doesn't need access to payroll files, and Finance doesn't need access to social media accounts.

Step 5: Create a Simple Approval Process

- [ ] **Require manager or owner approval before granting new access.**

Without an approval step, employees often collect permissions they don't really need. Over time, this "access creep" becomes a security risk.

Keep it simple. If someone needs new access, they should send a quick email or ticket with a reason. A manager or the business owner approves it before IT grants it. Even in as small as a 4-person team, this step adds accountability.

Step 6: Review Access Regularly

- [ ] **Check who has access every 3–6 months. Remove what's no longer needed.**

Roles change, people leave, and projects end. Access that made sense six months ago might now be a liability. Regular reviews keep permissions aligned with reality.

Export access reports from your main systems (most business software lets you do this). Sit down with your managers and ask: "Does this person still need this?" Remove accounts for ex-employees immediately.

Step 7: Keep Admin Accounts Rare

- [ ] **Limit admin or "all access" accounts to the bare minimum.**

Admin accounts can change settings, access all data, and bypass controls. If one gets hacked, the attacker has the keys to your business.

List out who currently has admin access. Decide who truly needs it (usually just the owner or IT lead). Downgrade everyone else to standard accounts.

Step 8: Seperate Critical Duties

- [ ] **Make sure no single person controls an entire critical process.**

Fraud, mistakes, or simple oversight are less likely when two people share responsibility. For example, one person should approve invoices, and another should pay them.

Review financial and operational workflows. Identify any areas where one person has too much control and split responsibilities between two people.

Step 9: Use Temporary Access As Needed

- [ ] **Grant short-term access for projects, then remove it.**

Temporary access prevents long-term risk. Without this step, people keep privileges they don't need long after a project ends.

When granting access, set a reminder to revoke it after the project ends. Many tools let you set expiration dates automatically but a calendar reminder works fine too.

Step 10: Monitor Key Activities

- [ ] **Keep records of sensitive actions (like payroll edits or bank account changes).**

Logs act like a security camera for your systems. If something goes wrong, you can see who did what and when. They also deter misuse because employees know actions are tracked.

Most business apps (QuickBooks, HR systems, CRMs) have built-in logging. Check settings and turn on activity tracking where available. Review logs occasionally for unusual behavior.

Step 11: Add Basic Safeguards

- [ ] **Strengthen security with simple technical tools.**

Even small measures make a big difference in reducing risk, especially for high-value accounts like payroll or banking.

- Turn on multi-factor authentication (MFA) wherever possible. Start with admin accounts.
- Store logins in a password manager instead of spreadsheets.
- Limit device permissions (e.g., don't allow everyone to install apps or use USB drives).

The Principle of Least Privilege isn't to make life harder for your team, it's about protecting the business you've worked hard to build. By working through this checklist, step by step, you'll reduce the chances of costly mistakes, keep sensitive information safe, and show your customers and partners that you take security seriously.