TechpioAsset

User Registration & Role Testing Guide

Version 1.3 · 7 August 2026 · applies to piotask.com · covers all 13 system roles

This guide explains every way a user account can be registered in TechpioAsset, how roles are assigned, and gives a ready-to-run test script for each role with a suitable example persona. Follow it top to bottom for a full access-control regression pass, or jump to one role to verify a single account.

1. How user accounts are registered

TechpioAsset is invitation-only by design: there is no public self-signup, so no stranger can create an account on your tenant. Accounts come into existence in one of four ways, and the first is the everyday one.

1a. Inviting a user from the People page (the everyday way) — NEW

Who can do this: Super Admin and Company Admin (full user managers) — and HR. HR may invite Registered Employees only: registering a joiner is HR work, granting privileged roles is not, and the server refuses any other role from an HR invite. Nobody else sees the button.

The full process, step by step:

- 1. Sign in as a Super Admin or Company Admin and open People (Administration group).
- 2. Click “Invite user” (top right, next to Export).
- 3. Fill in first name, last name and work email. Job title, department and office are optional and can be set later; department matters because it drives the DEPARTMENT data scope.
- 4. Tick one or more roles. Registered Employee is pre-ticked — least privilege unless you decide otherwise.
- 5. Click “Send invitation”. Two things happen: the person is emailed a link, and the same link is shown to you ONCE with a copy button — hand it over on chat or in person if your company has no email delivery configured.
- 6. The account now appears in People with status “Invited”. It cannot sign in yet: its password is a random placeholder nobody knows.
- 7. The invitee opens the link (valid 7 days, single use), chooses their own password (minimum 12 characters), and clicks “Activate my account”. That one step sets the password, verifies the email, and flips the account to Active.
- 8. They sign in at piotask.com/login. Done — no administrator ever knew or typed their password.

Example: Kavita (Super Admin) invites Meera Iyer, meera@sunrisetextiles.in, as Registered Employee in Engineering. Meera gets the email on her phone, sets her password over lunch, and raises her first laptop request the same afternoon.

If a link expires or goes astray: open the person in People → Manage → “Resend invitation”. A fresh 7-day link is emailed and shown to you once — and the old link stops working the moment the new one exists, so exactly one link is ever valid.

1b. Provisioning a tenant with its first Super Admin (site operator)

The platform operator (Site Administrator, e.g. admin@piotask.com) creates each customer company together with its bootstrap Super Admin.

- Sign in as the Site Administrator and open Platform → Tenants.
- Create the tenant: company name, plus the admin’s first name, last name and email.
- **The initial password is shown exactly once.** Copy it immediately and hand it to the customer over a secure channel; it cannot be retrieved again, only reset.
- That first user is a Super Admin and invites everyone else (see 1a).

Example: create tenant "Sunrise Textiles Pvt Ltd" with admin Kavita Rao, kavita.rao@sunrisetextiles.in. Kavita receives the one-time password, signs in, and is asked to set up her account.

1c. Automatic provisioning from your identity provider (SCIM)

For ongoing registration, connect your identity provider (Microsoft Entra ID / Azure AD, Okta, JumpCloud). New joiners then appear in TechpioAsset automatically and leavers are deactivated automatically.

- As a Super Admin, open Settings → Integrations and generate a SCIM token.
- In your IdP, add a SCIM provisioning app using the endpoint and token shown.
- Assign the IdP group (e.g. "All Employees") to the app; each member is created in TechpioAsset.
- Provisioned users sign in through SSO; they never need a TechpioAsset password.

Example: HR adds Rohit Sharma to the "All Employees" group in Entra ID on his joining day. Within the sync window he exists in People with the default Registered Employee role, and IT assigns his laptop against his account the same morning.

1d. Reactivating the built-in demo accounts (handy for role testing)

Your tenant ships with one seeded demo account per major role (employee@techpioasset.dev, finance@techpioasset.dev, auditor@techpioasset.dev, and so on). They are parked as Deactivated so they cannot sign in until you want them.

- Open People and switch the toggle at the top-right to Deactivated.
- Find the account for the role you want to test → Manage → Activate.
- Sign in with that account’s seeded demo password in a private/incognito window.
- When finished, deactivate it again so the directory stays clean.

Assigning and changing roles

- Open People → find the person → Manage.
- Details: name, job title, employee number, department and office (admin-only fields; department drives what the person can see under the Department data scope).
- Roles: tick one or more roles and Save. Conflicting combinations (e.g. raising and approving purchases) trigger a segregation-of-duties warning you must explicitly acknowledge.
- Account status: Activate / Deactivate, or Delete (a soft delete — the account disappears and can never sign in, but its asset-assignment history and audit trail are kept, and delete is refused while equipment is still assigned).

2. The 13 system roles

Every role carries a fixed permission set and a default data scope: ALL (whole company), DIRECT REPORTS (self + people they manage), or OWN (only their own records). Money is a special case: purchase prices, invoice values and budgets are visible only to Finance and Super Admin.

Role	What it is for	Data scope	Sees money?
Super Admin	**Full system access: users, roles, offices, workflows, platform settings.**	**ALL**	**Yes**
Company Admin	**Tenant owner: users, roles, workflows and configuration for the company.**	**ALL**	**No**
IT Administrator	**IT equipment, assignments, warranties, device lifecycle.**	**ALL**	**No**
IT Technician	**Executes IT work: deploy, assign, repair, maintain devices.**	**ALL**	**No**
HR	**Employees, onboarding and offboarding checklists.**	**ALL**	**No**

Office Administrator	**Furniture, kitchen equipment, pantry stock, office supplies.**	**ALL**	**No**
Finance	**Costs, invoice verification, purchase approvals, vendor spend, budgets.**	**ALL**	**Yes**
Procurement Manager	**Vendors, purchase requests/orders, RFQs, sourcing.**	**ALL**	**No**
Inventory Manager	**Stock, receiving (GRN), transfers, asset provisioning.**	**ALL**	**No**
Manager	**Reviews and approves requests raised by direct reports.**	**DIRECT REPORTS**	**No**
Registered Employee	**Views own assets, raises requests, reports damage, submits returns.**	**OWN**	**No**
Auditor	**Read-only: assets, invoices, approvals, audit log, reports.**	**ALL**	**No**
Vendor	**External supplier placeholder — no access until the vendor portal ships.**	**OWN**	**No**

3. Suitable example users for a test pass

Register these eight personas (via SCIM or by reactivating the matching demo account) to cover the roles that matter most day-to-day. Keep the naming pattern — role visible in the address — so test accounts are unmistakable.

Example person	Email	Role	Department
Kavita Rao	`kavita.sa@yourco.test`	**Super Admin**	**IT**
Arjun Mehta	`arjun.itadmin@yourco.test`	**IT Administrator**	**IT**
Priya Nair	`priya.finance@yourco.test`	**Finance**	**Finance**
Sofia D’Souza	`sofia.hr@yourco.test`	**HR**	**People**
Daniel Whyte	`daniel.mgr@yourco.test`	**Manager**	**Engineering**
Ravi Menon	`ravi.emp@yourco.test`	**Registered Employee**	**Engineering**
Grace Ferreira	`grace.audit@yourco.test`	**Auditor**	**Finance**
Tom Okafor	`tom.office@yourco.test`	**Office Administrator**	**Operations**

Make Daniel the manager of Ravi (People → Manage → Details) so the Manager approval path and the DIRECT REPORTS scope can be exercised for real.

4. Role-by-role test scripts

Each script assumes a fresh private-browser sign-in with that persona. "Should NOT" checks matter as much as the positive ones — a failed negative check is an access-control bug and should stop the release.

4a. Super Admin — Kavita

- Sign in. The sidebar shows every group, including Administration (People, Offices, Roles, Integrations, AI settings) and the Audit log.
- Open Settings → Offices: add an office "Pune Riverside" (code PUNE-01), then deactivate it. It must vanish from asset-form pickers but stay listed as Inactive on the Offices page.
- Open an asset: purchase price and current value are visible.
- Open People → Manage on Ravi: all sections present — Details, Roles, Account status, Delete.
- Security settings ask for your password again before showing 2FA and password controls.

4b. IT Administrator — Arjun

- Assets: can create an asset, assign it to Ravi, process a return.
- Should NOT see purchase prices or invoice values anywhere (money is Finance + Super Admin only).
- Should NOT see Roles or Platform in the sidebar.
- Maintenance: can raise and complete a work order.

4c. Finance — Priya

- Assets: purchase price and current value ARE visible.
- Invoices: can open an invoice, verify it, and see spend analytics under Insights.
- Budgets: can set a budget limit; a purchase request that exceeds it is refused with a clear message.
- Should NOT be able to manage users or roles.

4d. HR — Sofia

- People: can see everyone; can start onboarding for Rohit with a checklist template.
- Offboarding: starting one for a leaver lists their assigned assets to recover.
- Can invite a new joiner from People — the role is fixed to Registered Employee, and the form says so.
- Should NOT be able to invite anyone as IT Administrator or Super Admin — the server refuses it.
- Should NOT see invoice values or asset costs.

4e. Manager — Daniel

- Requests: sees "Awaiting me" when Ravi submits a request; can approve or reject it with a comment.
- People/assets visibility is limited to himself and his direct reports (DIRECT REPORTS scope) — searching for someone outside his team returns nothing.
- Should NOT be able to approve a request he raised himself (segregation of duties).

4f. Registered Employee — Ravi

- My assets: sees only equipment issued to him.
- My requests: raises "Replacement laptop"; it appears with status Submitted and moves as Daniel approves.
- Profile: can edit his own name, phone, job title. Department and office are read-only ("Set by your administrator").
- Should NOT be able to open People, Audit log, Offices, or anyone else’s asset. A direct URL like /people must show "not permitted", never data.

4g. Auditor — Grace

- Can open assets, requests, invoices, reports and the Audit log — everything read-only.
- The audit log shows the actions performed during this test pass (asset assigned, office created, user deleted) with actor and before/after values.
- Should NOT see any Create/Edit/Delete buttons; attempts via direct API calls are refused.

4h. Office Administrator — Tom

- Inventory: can receive pantry/office stock, adjust levels, transfer between locations.
- Can manage furniture and office-supply assets; should NOT see IT cost data or user management.

5. How assets are added — step by step

Who can add assets: roles holding assets:create — IT Administrator, Office Administrator, Inventory Manager and Super Admin. Purchase price and value fields are visible only to Finance and Super Admin; everyone else records the asset without money.

Path A — add one asset by hand

- 1. Open Assets and click “Add asset” (top right).
- 2. Fill the required fields: a name (“Dell Latitude 5440”), a short unique asset tag (“AST-0201”), a category (Laptop, Furniture, …) and its condition.
- 3. Add what you know: brand, model, serial number, office, purchase date, warranty end date. Serial numbers make discovery reconciliation automatic later.
- 4. Save. The asset appears in the Assets list immediately as available stock.
- 5. To hand it to a person: open the asset → Assign → choose the user, condition out and any accessories. The assignee sees it under “My assets” and acknowledges receipt; every assignment and return is kept forever as history.

Path B — bulk import from Excel

- 1. Assets → “Import Excel”. Download the template, fill one row per asset.
- 2. Upload; the preview flags problems (duplicate tags, unknown categories) before anything is written.
- 3. Confirm. Bad rows are reported, never silently skipped.

Path C — automatically from purchasing (the procurement loop)

- 1. Anyone raises a purchase request (“3 laptops for the new joiners”); the approval chain (manager, Finance above threshold) runs.
- 2. Procurement converts the approved request to a purchase order and issues it to the vendor.
- 3. When boxes arrive, the receiver records a goods receipt (GRN) against the PO — quantities, serials, location.
- 4. Individually-tracked lines (laptops, monitors) become asset records automatically, one per unit, each traceable back to its receipt line; consumables go into stock with lot and expiry tracking instead.
- 5. Finance three-way-matches invoice vs PO vs receipt before payment; a mismatch needs an explicit, audited override.

Use Path A for odd one-offs, Path B for migrating an existing register, Path C for everything you buy from now on — it keeps the paper trail from request to laptop-in-hand with no retyping.

6. Cross-cutting checks (any role)

- Two-factor authentication: Profile → Security settings → confirm password → scan the QR code with Google Authenticator/1Password → enter the 6-digit code. Sign out and back in: the code is now required. Disabling needs password AND a current code.
- Wrong password at the security gate must be refused and the page must stay hidden.
- Soft delete: delete a test user who has returned all equipment. They vanish from People (both views) and cannot sign in, but their past asset assignments still show on each asset’s history, answering "who had this laptop".
- Delete refusal: deleting a user who still holds an asset must fail with "…assets are still assigned to this user".
- Deactivated view: deactivated accounts appear only under People → Deactivated, never in the default list; CSV export follows whichever view is open.
- Notification preferences: Profile menu → Notification settings. Optional types can be switched per channel; mandatory ones (Approval required, Request rejected) are locked visibly and refuse changes at the API too.

7. Best recommendations (from our side)

1. The invite flow is now live — use it as the default registration path. Shipped in this release: People → Invite user, exactly as documented in section 1a, with a 7-day single-use link and the invitee choosing their own password. “Resend invitation” is also live on Invited accounts, and HR now holds the invite right — restricted to Registered Employees, so registering joiners is self-service for HR while privileged roles stay with user managers.

2. Enforce two-factor authentication for admin roles. The 2FA experience is now complete (QR, password-gated settings). Require it for Super Admin, Company Admin and Finance — the accounts that can move money visibility and access.

3. Use the demo accounts as a permanent role-testing rig. Keep them deactivated in daily use; reactivate the one you need, test, deactivate again. Never grant a real person a second role "just to check something" — use the matching test persona instead, so the audit log stays honest.

4. Run the negative checks every release. The most expensive access bugs are the ones where someone sees too much. Sections 4b, 4e, 4f and 4g each carry a "Should NOT" line — those eight checks take ten minutes and cover the cost-visibility rule, both restricted scopes, and read-only enforcement.

5. Complete the operational safety net. Off-site database backups (S3 credentials) remain the one open operational risk: today the on-server backup is the only copy. This is configuration, not code, and is ready to switch on as soon as credentials are provided.