Make Your MIP Permissions Audit-Ready in Hours

***Last Security Review Date:* ____________________________**

Use this worksheet to design, test, and document a rock-solid MIP Fund Accounting security model. Tick each task, list the owner, and file the finished PDF in your audit folder.

Step 1 — Map Duties & Segregate Roles (≈ 1 hr)

Task	**✔**	***Owner / Notes***
Diagram who enters, approves, and reconciles AP, AR, Payroll, GL	□	__________
Flag conflicts (same person in two boxes)	□	__________
Freeze the duty map for reference	□	__________

Step 2 — Build Core Security Groups (≈ 2–3 hrs)

Group	*Rights Snapshot*	✔	*Owner*
AP Clerk	*Add invoices, no Posting*	□	__________ _
AP Approver	*Approve/Post only*	□	__________ _
Payroll Reviewer	*View payroll reports*	□	__________ _
Fiscal Admin	*All finance, no system utilities*	□	__________ _
Auditor RO	*Read-only to needed reports*	□	__________ _

Step 3 — Apply Least-Privilege Rights

Task	✔	Owner / Notes
Menus – uncheck unused modules	□	___________
Tasks – grant Add/Edit only where required; avoid Delete	□	___________
Report Access – restrict payroll folders from AP staff	□	___________
Disable shared/full-access IDs	□	___________

Step 4 — Test with Dummy Users (≈ 30 min)

Task	✔	Owner / Notes
Create one test user per group	□	___________
Walk through daily tasks; log missing rights	□	___________
Fix gaps by editing the group, not individual IDs	□	___________

Step 5 — Enable Tracking & Archive Evidence (≈ 1 hr)

Task	**✔**	***Owner / Notes***
Turn on Login Tracking (Admin › Organization)	□	___________
Export Security Rights report (PDF) per group	□	___________
Save report & duty map to Audit folder (quarterly)	□	___________

Advanced Hardening (Optional)

- *MIP Cloud Two-Factor Authentication → □ Owner ___________*
- *Password policy: 12 chars, rotate 90 days → □ Owner ___________*
- *Annual July permission review (calendar invite) → □ Owner ___________*
- *Cross-train so two staff cover each critical role → □ Owner ___________*
- *On-prem SQL row security for segment-level lockdown → □ Owner ___________*

Common Pitfalls & Quick Fixes

Pitfall	***Impact***	***Fast Fix***
“Full Rights” for everyone	***Zero audit trail***	***Move to group-based least privilege***
Inactive IDs left enabled	***Ghost logins, fraud risk***	***Disable ID at termination***
Generic “Audit” login	***Blurred accountability***	***Create named read-only auditor IDs***

Time Budget—Complete Overhaul in < 1 Day

Task	***Est. Time***
Duty mapping workshop	***1 hr***
Group creation & rights setup	***2–3 hrs***
User reassignment	***30 min***
Testing & documentation	***1 hr***
Total	***< 1 business day***

Why Tight Security Pays Off

- *Protect Sensitive Data: Donor, payroll, grant budgets.*
- *Fraud Prevention: Clear segregation of duties.*
- *Audit Speed: Hand auditors a PDF—no live screen-shares.*
- *Regulatory Compliance: GAAP, Uniform Guidance, internal control frameworks.*

Need an Expert Hand?

McGovern Consulting Group audits, designs, and maintains role-based security for nonprofits and governments every year.

- *Audit of current rights & risks*
- *Scalable security-group blueprint*
- *Staff training & quarterly reviews*