DOCUMENTO PUBBLICO · 2026-09-21

Matrice dei permessi per ruolo

Ruoli, permessi e separazione dei compiti

SEMPI S.r.l. — Società Benefit
Terrazza Solferino, Via Davide Bertolotti n. 7, 10121 Torino (TO), Italia
P. IVA IT12315280011 · REA TO-1280911 · PEC sempi@legalmail.it

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati.

Role-Based Access Control (RBAC) Matrix — ISO27001 + Separation of Duties

Version: 1.0.0

Effective: 2026-07-14

Owner: Compliance Officer (Claude)

ROLES & PERMISSIONS

Role Hierarchy

```
┌─ OWNER (All permissions)
│  └─ ACCOUNTANT (majority of operations)
│  ├─ CLERK (operational only)
│  └─ VIEWER (read-only)
└─ AI_BOT (ARYA — limited to invoice draft creation + read reports)
```

Permission Definitions

Permission	Description	Risk	Review Frequency
---	---	---	---
`EDIT_INVOICES`	Create, edit, delete invoices & purchase orders	HIGH	Monthly
`MANAGE_CLIENTS`	Create, edit, merge, delete customers & suppliers	HIGH	Quarterly
`VIEW_REPORTS`	Read financial reports, tax registers, trial balance	MEDIUM	Quarterly
`EDIT_COMPANY`	Modify company settings, close fiscal year, chart of accounts	CRITICAL	Annually
`EXPORT_DATA`	Export CSV/PDF (triggers audit log + Sentry)	MEDIUM	Quarterly
`MANAGE_USERS`	Create/revoke user accounts, assign roles	CRITICAL	Quarterly
`ACCESS_AUDIT_LOG`	View audit trail (security-sensitive operations)	CRITICAL	Quarterly

---

RBAC MATRIX

Feature	Owner	Accountant	Clerk	Viewer	AI_BOT
---	:---:	:---:	:---:	:---:	:---:
INVOICING					
Create invoice	✅	✅	✅	❌	✅ (draft only)
Edit invoice	✅	✅	✅	❌	❌
Delete invoice	✅	✅	❌	❌	❌
Post to ledger	✅	✅	❌	❌	❌
Export invoice PDF	✅	✅	✅	❌	❌
JOURNAL ENTRIES					
Create entry	✅	✅	❌	❌	❌
Edit entry	✅	✅	❌	❌	❌
Delete entry	✅	❌	❌	❌	❌
Post entry	✅	✅	❌	❌	❌
CUSTOMERS & SUPPLIERS					
Create client	✅	✅	✅	❌	❌
Edit client	✅	✅	✅	❌	❌
Delete client	✅	❌	❌	❌	❌
Merge duplicate clients	✅	❌	❌	❌	❌
View payment terms	✅	✅	✅	✅	❌
FINANCIAL REPORTS					
View trial balance	✅	✅	❌	✅	✅ (read-only)
View balance sheet	✅	✅	❌	✅	✅ (read-only)
View P&L	✅	✅	❌	✅	✅ (read-only)
Export bilancio to File	✅	✅	❌	✅	❌
VAT COMPLIANCE					
View VAT registers	✅	✅	❌	✅	❌
Liquidate VAT	✅	✅	❌	❌	❌

File VAT return	✅	✅	❌	❌	❌
COMPANY SETTINGS					
Edit company details	✅	❌	❌	❌	❌
Manage chart of accounts	✅	❌	❌	❌	❌
Close fiscal year	✅	❌	❌	❌	❌
USER MANAGEMENT					
Create user	✅	❌	❌	❌	❌
Assign role	✅	❌	❌	❌	❌
Revoke user access	✅	❌	❌	❌	❌
View audit log	✅	✅	❌	❌	❌
AI FEATURES					
Enable/disable ARYA	✅	✅	❌	❌	N/A
Review ARYA suggestions	✅	✅	✅	❌	N/A
Accept ARYA draft	✅	✅	✅	❌	❌

SPECIAL CASES & EXCEPTIONS

Separation of Duties (Anti-Fraud Control)

Rule: No single user can both CREATE and APPROVE a payment.

Implementation:

- Invoice creator cannot post to ledger (different user required)
- VAT liquidation creator cannot file VAT return (different user required)
- Bank reconciliation matching cannot be performed by payment creator

Enforcement: Code-level check before action (test: `tests/compliance/separationOfDuties.test.ts`)

Consultant Access (External Accountant)

Scenario: Studio XYZ hires an external accountant for Q3 audit.

Access Level: ACCOUNTANT role, but with restrictions:

- ✅ Can view invoices, reports, trial balance
- ✅ Can create journal entries (audit adjustments)
- ❌ Cannot delete entries or close fiscal year
- ❌ Cannot access user management or company settings

Enforcement:

- Time-limited access (expires on end date)
- Cannot grant new permissions (Owner approval required)
- Audit log flags consultant access (`consultant_name: 'external'`)

MULTI-TENANT ISOLATION (Critical for Compliance)

Rule: User in Company A must NOT access Company B's data.

Enforcement Layers:

1. **Database Schema Isolation:**

- Each company has separate PostgreSQL schema

- User authentication tied to `company_id`

- Queries always filtered by `company_id` (Drizzle middleware)

2. **Middleware Guard (Express):**

`typescript

// server/middleware/tenantMiddleware.ts

app.use((req, res, next) => {

const companyId = req.user?.companyId;

const requestedCompanyId = req.params.companyId || req.body.companyId;

if (companyId !== requestedCompanyId) {

return res.status(403).json({ error: 'Access denied' });

}

next();

});

`

3. **Application Logic:**

- Every query includes `WHERE company_id = $1`

- JOIN operations respect company boundaries

- Exports (CSV/PDF) only include own company's data

4. **Test Coverage:**

- `tests/compliance/multiTenantIsolation.test.ts` — attempt cross-tenant access → 403

- Run on every merge

PRIVILEGE ESCALATION PREVENTION

Attack	Prevention	Test
---	---	---
User modifies token to elevate role	JWT signature verification (RSA-256)	`jwtValidation.test.ts`
SQL injection to bypass RBAC	Parameterized queries (Drizzle)	`sqlInjection.test.ts`
Direct DB access to bypass app logic	VPC isolation (no public DB endpoint)	Manual verification
Cookie tampering	Secure flag (HTTPS-only) + HttpOnly	`tests/compliance/cookieSecurity.test.ts`
Cross-tenant cookie reuse	Session tied to company_id + IP	`multiTenantIsolation.test.ts`

PERIODIC REVIEW & AUDIT

Monthly Review

- Check for orphaned users (no company assigned)
- Verify no stale API tokens
- Audit log: review failed login attempts

Quarterly Review

- Access matrix review (any changes needed?)
- Permission usage audit (who is using MANAGE_USERS?)
- Consultant access: verify time limits

Annually

- Full RBAC penetration test (external auditor)
- Review for privilege creep (did roles expand over time?)
- Update separation of duties rules if needed

COMPLIANCE CHECKLIST

- [ ] RBAC matrix reviewed quarterly
- [ ] Separation of duties enforced (code-level checks)

- [ ] Multi-tenant isolation tested (every merge)
- [ ] JWT signature verification active
- [ ] Consultant access time-limited
- [ ] Audit log includes role changes
- [ ] Failed access attempts logged
- [ ] Annual penetration test scheduled

Owner: Compliance Officer (Claude)

Last Reviewed: 2026-07-14

Next Review: 2026-10-14

Status: ACTIVE

> **Sorgente:** docs/compliance/RBAC_MATRIX.md
> **SHA-256 del sorgente:** 36140451b2ceee124bb5f7fa38d21c9e43f3eb547c4344f76c488d070f048f9b
> La data certa di questo documento è data dalla marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014). L'impronta qui sopra identifica il testo di partenza nel repository.