



SECURE CUSTOM FIELDS FOR JIRA

Jira doesn't protect individual fields. This does.

Add field-level view and edit permissions to your Jira custom fields; So sensitive data stays private without splitting your workflows.

Free 30-day trial

on the Atlassian Marketplace

THE GAP

Jira's permission model controls access to projects and issues, not to individual fields within an issue. Any user who can open an issue can see **everything on it**: salary figures, legal details, budget data, and anything else in a custom field.

Separate projects, internal comments, fields pulled off screens; the usual workarounds aren't access controls. **Field-level security is.**

ISSUE TA-2208 · Senior Offer

ONE ISSUE

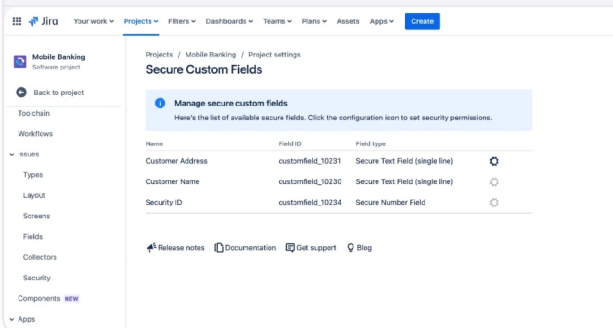
	RECRUITER	ENGINEER
Candidate	A. Rivera	A. Rivera
Stage	Offer	Offer
Base salary	\$185,000	***** RESTRICTED
Equity grant	4,000 RSU	***** RESTRICTED
Background check	Cleared	***** RESTRICTED

Same issue · the right visibility for every user

THE FIX

One issue. The right visibility for every user.

Apply view and edit permissions directly to individual custom fields. Each user sees only what they're authorized to. Sensitive data stays protected, the rest of the issue stays visible, and workflows stay intact.



Capabilities

01

Field-Level Permissions

Control who can view or edit each field by user, group, or role, independent of project and issue permissions.

02

Configurable Data Protection

Unauthorized users see the field label but never the value. Configure masked display where appropriate.

03

AES-256 Encryption

Sensitive field data encrypted at rest and in transit. Protection at the data layer, not just the interface.

04

Audit-Ready Access Logs

A timestamped record of who viewed or modified each sensitive field; the evidence layer compliance needs.

05

Automation Compatible

Existing automation rules, CSV import/export, and REST API integrations keep working without modification.

06

Project-Level Delegation

Project admins set local field permissions under global guardrails. Governance at scale, no bottlenecks.

Where teams use it

HR Operations

Salary, ratings, and employee records visible only to authorized HR roles and line managers.

Legal & Contracts

Settlement amounts, privileged notes, and risk classifications restricted to legal roles.

Finance & Audit

Budget figures and approval thresholds visible to finance management only.

IT & Service Desk

Internal diagnostic notes and credentials restricted to senior engineers.

Built for regulated environments.

Field-level access control, encryption, and audit logs align Jira with the frameworks your team is already accountable to.

FRAMEWORK	RELEVANT REQUIREMENT
GDPR	Data minimization & purpose limitation; Personal data accessible only to users with a legitimate need.
SOC 2	Logical access controls based on the least-privilege principle (CC6).
ISO 27001	Information access restrictions aligned to access control policy (Annex A, Control 8.3).
HIPAA	Technical safeguards for access to sensitive operational and patient-adjacent data.

+ Available in Atlassian Government Cloud – FedRAMP® Moderate authorized.

● Built on Atlassian Forge

Your data never leaves Jira Cloud infrastructure. No external data storage, no third-party data transfer.

● On the Atlassian Marketplace

Free 30-day trial. Trusted by teams in healthcare, financial services, legal, and regulated industries worldwide.



Platinum
Solution Partner
ENTERPRISE



Gold
Marketplace Partner

TRUSTED BY TEAMS AT

HONDA

RioTinto

S&P Global



“Unauthorized users were setting field values meant to gate our approvals. With this app we added specific user and group permissions on the field and built it right into the workflow validation.”

WARREN KENT · ATLASSIAN MARKETPLACE REVIEW

GET STARTED

Try Secure Custom Fields for Jira free for 30 days.

Scan to start your trial or request a guided demo.



START TRIAL



REQUEST DEMO

RSRICKSOFT

Ricksoft, Inc.

800 West El Camino Real, Suite 180, Mountain View, California 94040, USA

ricksoft-inc.com