

COMPLIANCE & SECURITY · TEMPLATE

Access Control and Offboarding Policy Template

For founders and operations leaders who need a clear, adoptable policy for granting, reviewing, and removing system access.

How to use this: Define your roles and access map first, then use the offboarding checklist as a same-day procedure whenever someone leaves or changes roles.

Role Definitions and Access Levels

Define the roles that exist in the company and what each should be able to access, independent of the specific people currently in them.

Role	Systems They Need Access To	Access Level (View / Edit / Admin)	Approved By
Engineering			
Sales / Customer Success			
Finance / Billing			
Support			
Admin / Founder			

Current Access Map

List every system that holds sensitive data or controls, and who currently has access to it.

Production infrastructure / cloud environment: who has access?

Code repositories: who has access?

Customer data platform / CRM: who has access?

Billing and financial systems: who has access?

Email and core communication tools: who has admin rights?

Access Request and Approval Process

- ☐ New access requests are submitted to a named approver, not granted informally.
- ☐ Access is granted at the minimum level needed for the person's role.
- ☐ Temporary or contractor access has a defined expiry date set at the time it's granted.
- ☐ Shared logins are avoided in favour of individual, attributable accounts wherever possible.

Quarterly Access Review

- ☐ Review the full list of who has access to production systems.
- ☐ Review the full list of who has access to customer data.
- ☐ Confirm every admin-level account is still necessary and still an active employee.
- ☐ Remove or downgrade any access that no longer matches the person's current role.

Same-Day Offboarding Checklist

Complete every item on the employee's last working day, not after.

- ☐ Disable or remove email and core communication tool access.
- ☐ Remove access to code repositories and production infrastructure.
- ☐ Remove access to customer data platforms, CRM, and support tools.
- ☐ Remove access to billing, finance, and admin systems.
- ☐ Revoke or rotate any shared credentials, API keys, or tokens the person had access to.
- ☐ Retrieve or remotely wipe company-managed devices.
- ☐ Confirm removal with a second person and log the date completed.