Access Control Policy

NORTHSTAR WORKSHOP | WORKED EXAMPLE

Company: Northstar Workshop
Owner: Rowan Ellis, IT lead
Approver: Avery Lane, Managing Director
Effective: 15 October 2026 | Version: 1.0
Next review: 15 October 2027

Purpose and scope

This policy covers employee, contractor and service accounts that access the workshop’s order system, cloud documents and managed devices.

Account requests

Managers request access in the service desk. The IT lead verifies the role and system owner approval before provisioning a named account.

Sign-in and privileged access

Staff use central sign-in and multifactor authentication. Administrators use separate privileged identities. The IT lead documents service accounts and records any exception in the access register.

Review and offboarding

System owners review account access quarterly. IT disables accounts by the scheduled departure time, revokes active sessions, and records completion in the offboarding ticket.

Evidence and review

Retain access approvals, quarterly review exports and offboarding records in the restricted security evidence folder. The IT lead reviews the policy annually or after a material change to access systems.

About this example

Northstar Workshop and its staff are fictional. Use the example to see the expected level of detail, then adapt the draft to your own approved practices.