POLICY

Access Control Policy

Who gets access to what, how it is granted, reviewed and removed

Document owner	[Owner name and role]
Approved by	[Approver name and role]
Version	[1.0]
Effective date	[Date]
Next review	[Date, at least yearly]
Classification	[Internal]

Purpose

This policy sets the rules for granting, using, reviewing and removing access to [Company Name] systems and information. Its goal is that only the right people and services have access, only to what they need, and only for as long as they need it.

Scope

This policy applies to:

- All employees, contractors and third parties with access to [Company Name] systems.
- All user accounts, privileged accounts, service accounts, API keys and tokens.
- All systems that store or process company or customer data, including the [identity provider, e.g. Google Workspace or Okta], cloud platforms in [AWS / GCP / Azure], source code in [GitHub], production databases, SaaS applications and company devices.

Roles and responsibilities

Role	Responsibilities
[IT Manager]	Owns this policy. Manages the identity provider, SSO and MFA settings, provisioning and deprovisioning. Runs access reviews.

Role	Responsibilities
[Engineering Lead]	Manages access to cloud infrastructure, production and source code. Owns service accounts used by engineering.
System owners	Approve access requests for their systems, define roles and complete access reviews on time.
Managers	Request access for their team members and report role changes and departures to [People Operations] the same day they are known.
[People Operations Lead]	Triggers joiner, mover and leaver workflows from the [HR system].
[Security Lead]	Monitors compliance, approves exceptions and reviews privileged access.
All users	Protect their credentials, use MFA, and never share accounts.

Policy statements

Identity and single sign-on

1. Each person must have one unique, named user account. Shared user accounts must not be used, except documented break glass accounts (see statement 24).
2. The [identity provider] must be the source of user identity for all systems that support SSO, meaning single sign-on, where users log in once through a central provider.
3. New SaaS applications that store confidential data must support SSO, or the [Security Lead] must approve an exception before purchase.
4. User accounts must be created only from an approved request recorded in [ticketing tool] or an automated workflow from the [HR system].

Authentication

5. MFA must be enforced in the [identity provider] for all users, with no option to skip enrollment.
6. Phishing-resistant MFA, such as passkeys or hardware security keys, must be used for administrator accounts and access to production cloud consoles.
7. SMS codes must not be used as an MFA factor, except as a temporary recovery method approved by the [IT Manager].
8. Systems that cannot use SSO must enforce their own MFA where available.

Passwords and passkeys

9. Passkeys should be used wherever a system supports them. Where passwords are still needed, they must have at least [14] characters and must not be reused across systems.

10. Passwords must not be forced to change on a fixed schedule. They must be changed immediately when there is any sign of compromise.
11. Staff must store passwords that are not covered by SSO in the company password manager, [1Password / Bitwarden]. Passwords must not be stored in documents, spreadsheets, chat messages or browser storage outside the password manager.
12. Initial and reset passwords must be unique, sent through a secure channel and changed at first use.
13. Accounts must lock or slow down after [10] failed login attempts.

Least privilege and role-based access

14. Access must be granted on a need to know and least privilege basis. Users must receive only the access needed for their role.
15. Access must be granted through groups or roles defined in the [identity provider] or cloud IAM, not assigned to individuals one by one, where the system allows it.
16. System owners must keep a role matrix that lists standard access for each team, stored in [location].
17. Access to production customer data must be limited to named roles approved by the [Engineering Lead] and must be logged.

Joiners, movers and leavers

18. **Joiners.** Standard access must be provisioned on or before the start date from the role matrix. Extra access must have a separate approved request.
19. **Movers.** When a person changes role, the manager must request new access and the old access that is no longer needed must be removed within [5] business days.
20. **Leavers.** Access to the [identity provider] must be disabled within [4 hours] of the end of employment, or immediately for involuntary terminations. All remaining accounts, tokens and keys must be removed or transferred within [2] business days.
21. Company devices must be returned or remotely locked through the [MDM] on the last working day.
22. Each joiner, mover and leaver action must be recorded in [ticketing tool] with dates and approvals.

Privileged access

23. Privileged access, such as cloud administrator, identity provider administrator, database administrator or GitHub organization owner, must be limited to the smallest number of people needed, listed in the [privileged access register].
24. Administrators must use a separate privileged role or account for administrative tasks. Break glass accounts must have strong credentials stored in a sealed vault, must alert the [Security Lead] when used, and must be tested every [6 months].
25. Production access should be granted just in time for a limited period, through [AWS IAM Identity Center / GCP PAM / access request tool], and expire automatically after [number] hours.

26. All privileged actions in cloud platforms and the [identity provider] must be logged, and logs must be kept for at least [12 months].

Access reviews

27. System owners must review user access to in-scope systems at least every [quarter] for privileged and production access, and every [6 months] for other in-scope systems.
28. Reviews must check that every account belongs to a current person or approved service, and that access still matches the role.
29. Access that is not justified must be removed within [5] business days of the review.
30. Each review must be recorded with the reviewer, date, list reviewed and changes made, in [ticketing tool / compliance platform].

Service accounts and secrets

31. Each service account must have a named owner, a documented purpose and only the permissions it needs, recorded in the [service account inventory].
32. Service accounts must not be used for interactive login by people.
33. Secrets such as API keys, tokens and passwords must be stored in [AWS Secrets Manager / GCP Secret Manager / Vault], never in source code or configuration files in repositories.
34. Short-lived credentials, such as cloud workload identities or OIDC federation for CI pipelines, must be used instead of long-lived keys where supported.
35. Long-lived secrets must be rotated at least every [12 months] and immediately when a person with access leaves or a leak is suspected.
36. Repositories must use secret scanning, such as [GitHub secret scanning], and detected secrets must be revoked within [24 hours].

Remote and network access

37. Access to administrative interfaces and internal services must require SSO and MFA, through [zero trust access tool / VPN], and must not be open to the internet without authentication.
38. Access to company systems from devices not managed by the [MDM] must be blocked or limited to [browser-only access to approved apps].

Exceptions

Exceptions must be requested in [ticketing tool] with the business reason, risk and compensating controls. The [Security Lead] and the system owner must approve them. Exceptions must have an end date no later than [6 months] and must be recorded in the [exceptions register].

Enforcement

Violations, such as sharing credentials or bypassing MFA, may lead to removal of access and disciplinary action according to [Company Name]'s HR procedures. Compliance is checked through access reviews, identity provider reports, MDM reports and internal audits.

Related documents

- Information Security Policy
- Acceptable Use Policy
- Incident Response Plan
- [Role matrix]
- [Privileged access register]
- [Service account inventory]
- [Joiner, mover and leaver procedure]

Annex A mapping

Annex A control	Section that covers it
5.15 Access control	Least privilege and role-based access
5.16 Identity management	Identity and single sign-on
5.17 Authentication information	Passwords and passkeys, Service accounts and secrets
5.18 Access rights	Joiners, movers and leavers, Access reviews
5.3 Segregation of duties	Privileged access
6.5 Responsibilities after termination or change of employment	Joiners, movers and leavers
8.2 Privileged access rights	Privileged access
8.3 Information access restriction	Least privilege and role-based access
8.4 Access to source code	Least privilege and role-based access, Service accounts and secrets
8.5 Secure authentication	Authentication
8.15 Logging	Privileged access (statement 26)
8.18 Use of privileged utility programs	Privileged access

Annex A control	Section that covers it
8.20 Networks security	Remote and network access

Review and approval

The [IT Manager] must review this policy at least once every [12 months] and after major changes to identity systems, cloud platforms or the organization. Changes are approved by [Security Lead / Security Committee], recorded in the document control table and communicated to affected staff.