Access management and MFA policy

Policy | English · Template to adapt | v3.0 · 2026-10-16

Template version: 3.0. This policy assumes an approximately 80-person organization that may outsource IT, distinguishing business ownership from technical execution without requiring a dedicated identity team. Functions may be combined with deputies and suitable checks. Clauses become internal requirements only after adoption and do not describe controls as already implemented.

How to use this policy. Sections 1–5 state general rules. Apply scope and account categories in sections 6 and 8 before provisioning; use section 7 for personnel changes. Apply sections 9–10 before recovery or emergency intervention. Section 11 supports review; section 12 prepares adoption. Detailed sections are references for decisions before action, not steps postponed until the action is complete.

Type: policy for approval. This template proposes internal rules for granting, reviewing and withdrawing access. It becomes an organizational policy only after adaptation and approval. It is not a compliance attestation or an automatic selection of a legally required assurance level.

Purpose. Maintain justified, attributable and revocable access throughout its lifecycle, with risk-appropriate authentication. After adoption, “must” and “requires” express approved internal requirements; before adoption, every clause remains a proposal. The owner completes parameters, confirms available capabilities and removes any assertion of implementation that has not been verified. No clause states that the adopting organization already operates the proposed control.

Approval, scope and accountability

Field	Value to complete
Organization, reference, version	[TO COMPLETE: organization, reference, version]
Owner and approver	[TO COMPLETE: identity lead, management]
Approval and next review	[TO COMPLETE: dates]
Covered services and populations	[TO COMPLETE: staff, third parties, cloud, remote access]
Identity register and request process	[TO COMPLETE: systems, procedure]
Exception and emergency process	[TO COMPLETE: authorities, contacts]

Business managers justify need; resource owners authorize rights; the identity team applies and records changes. HR or supplier sponsors communicate authorized personnel changes. Security defines requirements and reviews exceptions. Each account holder protects authenticators and reports loss or unexpected prompts. These assignments must be reconciled with actual delegations and contracts so a named owner can accept each responsibility.

Service identities and shared accounts must be inventoried separately. Where individual interaction is possible, the organization favors a personal account. Any impossibility must identify an owner, compensating traceability and a reassessment date. Use of an account does not automatically prove which person acted. This distinction must remain visible when account activity is used in investigations.

1. Grant justified access

Each request states resource, rights, purpose, recipient, owner and duration. Requesters must not independently approve their own sensitive access. Role profiles must be limited to need. Temporary access must have a verifiable expiry. Copying all a colleague's rights does not replace a needs assessment. The approval record must explain any incompatible duties and the approved mitigation.

☐ Verify the recipient's identity and organizational relationship.

☐ Obtain the resource owner's approval.

☐ Identify incompatible duties: [TO COMPLETE: local rules].

☐ Set start, any end point and permitted use.

☐ Confirm actual rights applied, linked to the request.

Administrative access must use risk-appropriate identities and methods, separate from routine use where feasible. Avoid unnecessary permanent privileges; define temporary elevation and its records in [TO COMPLETE: administration procedure]. If a platform cannot support the chosen design, document the limitation and seek a bounded exception rather than claiming an unavailable capability.

2. Define MFA coverage

The organization requires MFA on [TO COMPLETE: resources, priority populations], with a coverage plan and exception checks. Methods must suit the service, users and risks. Prefer phishing-resistant mechanisms for sensitive access where available and deployable. Local requirements must identify accepted methods, recovery arrangements, owners and evidence of effective application.

NIST distinguishes assurance levels and authenticator properties. A manually entered code or an approved notification must not be presented as equivalent to phishing-resistant authentication. Select methods using their actual properties rather than a product's “MFA” label. This policy does not import every NIST assurance-level requirement into every service; any adoption of a specific level requires a separate applicability assessment.

Category	Local requirement	Owner and check
Administration and remote access	[TO COMPLETE: allowed methods, restrictions]	[TO COMPLETE: owner, coverage evidence]
Business applications	[TO COMPLETE: scope, rollout]	[TO COMPLETE: owner, frequency]
Incompatible services	[TO COMPLETE: compensation, dated exception]	[TO COMPLETE: decision maker, reassessment]

Disable authentication paths that bypass approved requirements after assessing dependencies. Check direct application access, external accounts and recovery methods as well. A configured rule that is not applied does not demonstrate coverage. Before rollout, confirm how exceptions and failures will be detected, and how users will obtain authorized assistance without creating an unmanaged bypass.

3. Enroll and recover securely

Initial enrollment, adding an authenticator and recovery require risk-appropriate identity verification. Support must not collect passwords or MFA codes. An urgent request from the affected account is insufficient authority for a reset. Use [TO COMPLETE: independent channel and checks] and record the operator. Confirm the new binding and the handling of lost or unauthorized methods with the responsible team.

Provide a controlled fallback for authenticator loss. Emergency accounts must be limited, protected, monitored and tested under [TO COMPLETE: scenario, frequency]. Activation triggers review. Store secrets and recovery codes in an authorized facility, separate from routine tickets. Availability arrangements must respect both accessibility and security needs; an unusable recovery process should be corrected rather than silently bypassed.

4. Review and withdraw

☐ For role changes, arrange an approved transition, remove unnecessary rights and bound any temporary overlap; verify essential access afterward.

☐ For departures, coordinate withdrawal at the authorized time.

☐ Examine groups, direct rights, delegation, third-party access and applications.

☐ Address sessions and tokens using mechanisms actually available.

☐ Have owners attest sensitive access at [TO COMPLETE: frequency].

☐ Assign due points and owners to identified anomalies.

For suspected compromise, use the relevant response playbook. Verify removal in the affected services; application sessions may need separate action. Preserve evidence of the result, not only the request. If a service or supplier cannot confirm removal, record the uncertainty, apply approved protections and escalate to the accountable owner.

5. Exceptions, monitoring and exercises

Every exception must state resource, risk, justification, compensating measure, decision maker, expiry and check. Renewal without examination is not risk management. Track effective MFA coverage, ownerless accounts, expired rights and unusual recoveries without inventing universal targets. Measures must state their assessed population and the limitations of the evidence collected.

Exercise a departure, role change and lost authenticator. The reviewer should be able to find who approved, what changed and how the result was verified. Review the policy after incidents, significant changes and at its planned review point. Determine record retention and applicable obligations with competent functions. No universal review interval or retention duration is asserted by this template.

Control requirements after adoption

Proposed internal reference	Requirement and evidence
ACC-01 — Granting	Sensitive access must retain an owner, justification and approval.
ACC-02 — Authentication	Owners must check effective MFA coverage and potential bypasses.
ACC-03 — Lifecycle	Personnel changes and temporary access must trigger review of rights and withdrawal results.
ACC-04 — Exception	Each exception must retain a risk-accepting authority, expiry, compensation and reassessment evidence.
ACC-05 — Internal assurance	Gaps must be tracked to verified correction or explicit acceptance of residual risk.

The process owner reports to [TO COMPLETE: body, frequency] on assessed coverage, ownerless access, expired exceptions and unverified withdrawals. Every indicator states scope and limitations; untested populations are not counted as compliant. Evidence remains available only to authorized people for a locally justified period.

Expired exceptions are reassessed by the designated authority; renewal is not implicit. If immediate removal threatens an essential activity, that authority decides a bounded transition and suitable protection. Policy changes must be approved, versioned and communicated to affected operators before implementation, except under an expressly defined emergency procedure.

6. Adoption scope and delegated authority

The owner must inventory covered directories, SaaS applications, remote access, administration consoles, backups and outsourced services. Include authorized supplier access and remote working. Personal equipment, industrial environments and special contractual arrangements require appropriate rules; this policy grants no authority beyond existing rights. List exclusions with their business owner and the decision needed to resolve them.

In a smaller organization, administration staff may notify personnel changes, management or business owners approve rights and an IT provider apply them. An MSSP may observe events without changing accounts. Every responsibility needs a holder, deputy, fallback channel and delegation boundary. A task without a confirmed executor is an adoption gap, not an available capability.

Decision	Internal owner	Execution and check
Open or change access	Resource owner	Provider/administrator; effective rights verified
Grant privilege or supplier access	Business sponsor and designated authority	Administrator; scope, duration and traceability checked
Restrict urgently	Coordinator within delegation	Authorized executor; effects and essential access checked
Accept exception	Named risk authority	Control owner; compensation and reassessment demonstrated

If the provider is unavailable, use backup contacts and contractual escalation. Record the inability to act and seek a business decision. Temporary measures must be authorized and achievable. After adoption, this policy prohibits turning uncontrolled shared access into a permanent solution merely because support is not responding. Document the safe work alternative or accepted interruption instead.

7. Joiners, movers and leavers

An authorized function must trigger the process: HR, management or a supplier sponsor. A direct email request is insufficient for sensitive access without independent approval of need. Record stable identity, role, resources, effective date, owner and any limit. Executors confirm created, refused and pending rights separately. An unfinished service must remain visible rather than being hidden under a completed general onboarding ticket.

Stage	Action and authority	Evidence and failure handling
Joiner	Verify identity, need and approved profile; prepare enrollment	Request linked to effective rights; do not grant unapproved sensitive access
Mover	Compare old/new roles; decide necessary overlap	Additions/removals recorded; temporary retention has owner/end
Leaver	Apply authorized timing/scope with business and IT	Rights and targeted sessions checked; inaccessible services remain pending
Supplier assignment ends	Confirm sponsor, accounts, delegation and exposed secrets	Access withdrawn/resources transferred; uncertainty escalated for risk decision

Before departure, decide who inherits operational responsibilities and information without handing the departing person's password to a replacement. Preserve needed data under approved rules, then check shared mailboxes, delegation, groups and applications. Account deletion is not a universal preservation method or proof that every external permission disappeared. Record each service's result and remaining provider dependency.

If urgent removal conflicts with continuity, the business owner chooses authorized alternative access or an accepted interruption. Every transition retains an end point, rights list and check. Later reactivation requires a fresh decision: assess current need rather than blindly restoring historical rights. Keep the approving person's rationale linked to the technical change.

8. Privileged, service, shared and supplier accounts

Privileged accounts must relate to justified administration tasks, with suitable operating environments and records. Holders distinguish routine work from administration. Where temporary elevation is available and selected, document approval, activation, duration and outcome. Otherwise, an exception must explain how standing privilege is controlled. Do not claim time-limited elevation where the platform or license does not support it.

A service identity must have a business owner, technical custodian and dependency list. Describe use, rights, authentication mechanism, secret or certificate storage and renewal. Do not label every identity MFA-covered merely because interactive accounts use MFA; check protection against the mechanism actually used. Include failure and recovery arrangements so secret changes do not unexpectedly stop an essential application.

Category	Parameters to complete	Expected check
Service or application	[TO COMPLETE: use, owner, dependencies, mechanism]	Protected secret, limited rights, testable renewal/stop
Exceptional shared account	[TO COMPLETE: justification, authorized holders, traceability]	Controlled secret access, stated attribution limits, holder departures tracked
Supplier	[TO COMPLETE: sponsor, contract, systems, timing/duration]	Need-based access, observable actions, confirmed withdrawal
Administration	[TO COMPLETE: tasks, rights, environment, approval]	Separated uses, privilege/anomaly review

A provider must not reuse a departed person's account without a decision. Equipment-imposed generic accounts require documented compensations such as network limits, controlled vault access, intervention records or monitoring. The risk authority approves traceability limitations. Do not present compensation as equivalent to individual identity when it cannot support that attribution. Preserve who used the available access route and what evidence exists.

9. MFA enrollment, loss and recovery

Before rollout, choose admitted methods, identify accessibility needs and plan replacement of lost authenticators. Test priority applications and alternative paths. Incompatible methods require an exception or approved working alternative, not indefinite invisible deactivation. Agree how users obtain assistance and how administrators detect bypasses before declaring the rollout operational.

Input	Authorized action	Evidence and limitation
New user	Verify identity; deliver instructions through controlled channel	Expected enrollment confirmed; no secrets in ticket
Lost method or replacement phone	Independent check, compromise assessment, approved recovery	Old method addressed, new one checked, named operator
Unexpected prompt	Report and assess account using playbook	Restriction decision or explanation; no default approval
Unavailable support	Defined backup and business decision	Request followed; no improvised sensitive access outside delegation

Recovery must not become a less controlled route than intended use. Support applies locally approved checks and must not base sensitive resets solely on urgency or a message from the affected account. If identity cannot be established through approved means, escalate and offer an alternative activity without asking for usable MFA codes. Explain the restriction to the requester through a trusted channel.

10. Emergency access and restoration of control

Define emergency scenarios: identity outage, loss of normal methods or inability to administer a critical service. Name authorized users, activation conditions, custody arrangements and necessary fallback access. Check that retrieval does not depend exclusively on the service it must rescue. Record how an authorized deputy can obtain assistance if the usual provider or approver is unavailable.

Microsoft's Entra emergency-access guidance recommends distinct authentication dependencies, protected custody, monitored use and post-use review. These principles inform this model; Entra-specific settings, account counts and review intervals are not universal values to copy into every environment. Test actual local mechanisms and retain the limitations rather than copying console settings without dependency analysis.

☐ Record reason, scope and operator before activation where urgency permits.

☐ Release capabilities only to authorized people through the defined channel.

☐ Record changes and preserve available activity evidence.

☐ Notify an independent recipient through the selected mechanism; keep delivery failure visible.

☐ After use, check rights, exposed methods, temporary access and normal operation.

☐ Revoke, replace or return capabilities to protected custody according to their nature and approved procedure.

☐ Have a reviewer examine necessity, authority and outcome; a lone operator must not claim independent assurance through self-approval.

11. Recertification, exceptions and evidence

Review the actual account/resource population rather than recent requests alone. Resource owners receive identities, rights, sponsors, available use information and exceptions. They decide retain, change, remove or investigate. No response is not approval: the coordinator follows up and escalates. Document excluded systems and explain how their owners will make a decision using available evidence.

Review record to copy	Value to complete
Population and coverage	[TO COMPLETE: systems, accounts, exclusions, extraction date]
Decision and authority	[TO COMPLETE: rights, need, owner, retain/remove]
Execution	[TO COMPLETE: provider, reference, date, result]
Gap	[TO COMPLETE: inability, compensation, accepted risk, end]

An exception identifies the unmet requirement, resources, rationale, alternatives, tested compensation, accepting authority and expiry. Set an early reassessment trigger such as role change, incident or a newly available capability. The owner verifies correction or obtains another decision; deleting a finding to improve a metric is not permitted. Keep local timing and retention choices explicitly approved.

12. Adoption and fictional exercise

Adoption has four gates: accepted inventory/responsibilities; tested requests/personnel changes; MFA, recovery and emergency checks on representative scope; gaps presented to the approver with resources and treatment plans. A signed policy without available executors or access is not successful acceptance. Set an effective date compatible with decisions still needed, and distinguish a pilot from general implementation.

Workshop-80, an entirely fictional organization, moves an employee from sales to finance. The sponsor requests accounting access; IT proposes copying an existing profile. Finance rejects wholesale copying, approves necessary tasks and authorizes limited overlap to finish orders. Fictional decision EX-A1 identifies rights, business check, owner and end point. None of the following records describes an actual adopter.

Fictional case	Decision	Acceptance evidence
Sales-to-finance move	Remove unnecessary rights; bound approved overlap	Before/after comparison and tested business operation

Fictional case	Decision	Acceptance evidence
Supplier staff departure	Sponsor confirms end; IT removes accounts/delegation	Verified results; unconfirmed external service separately tracked
Lost MFA method	Support follows independent verification and recovery	Old method addressed, new one validated, no codes in ticket
Emergency access drill	Authorized activation within agreed scope	Observable use, completed review, capabilities returned to control

Fail the exercise if a provider alone accepts business risk, a service account has no owner or access denial leads to secret sharing. Accept it when decisions and results can be located, unknowns are explicit and corrections have owners. Management retains the decision on remaining exceptions before general adoption; a passed scenario does not establish every untested system as compliant.

Working references

Also consult Microsoft emergency-access account guidance. Adapt technical requirements to the provider, actual permissions and local constraints.

NIST SP 800-63B-4 covers authenticators, assurance and recovery; its requirements do not automatically bind every organization. Microsoft access revocation documentation illustrates token and session limitations. Test proposed internal rules with your providers and adapt them to accessibility, continuity and security constraints.