

BREAK-GLASS ACCESS.

Break-glass accounts restore administrative access when normal sign-in, federation, or privilege activation fails. **A recovery path must survive the failed dependency, protect its credentials, and leave evidence of every use.**

- INDEPENDENT RECOVERY PATH
- PHISHING-RESISTANT AUTHENTICATION
- CONTROLLED CREDENTIAL CUSTODY
- TESTED EMERGENCY OPERATIONS

01 THE MECHANISM



A Reserved Recovery Identity

A dedicated emergency identity or role restores control when the ordinary administrative path is unavailable. **Reserve it for declared incidents and planned drills**; everyday administration and automation need their own identities. [07]



Independence Is the Test

Map the IdP, MFA, vault, network, device, and approval dependencies. A second account that needs the same failed service is not a second path. **Two credentials in one unavailable vault still fail together.** [08]



Strong Protection Still Applies

Use resilient, phishing-resistant authentication where supported, with controlled custody and usable backups. **Emergency access is not permission to remove all safeguards.** Test recovery mechanisms as carefully as primary credentials. [02] [06]

02 THE FLOW

Declare, Retrieve, Restore

ACTIVATE

1 **Declare:** identify the failed access path, incident lead, named operator, repair scope, and expected duration. Use a predefined alternate approval channel if normal tooling is unavailable.

2 **Retrieve:** follow the custody procedure from a designated secure workstation. Verify the real service URL and identity; record the custodian and operator without copying secrets into the ticket.

3 **Restore:** sign in through the prepared recovery path and perform only the necessary repair. Capture actions and changes; confirm that ordinary administrators can regain access.

Close, Review, Re-arm

RECOVER

1 **Close:** end emergency sessions, revoke temporary grants and tokens where supported, and remove incident-only policy changes. Preserve logs before closing the incident.

2 **Review:** reconcile operator actions, authentication events, approvals, and outcomes. Rotate disclosed or checked-out passwords; replace exposed credentials and validate stored copies.

3 **Re-arm:** return credentials to controlled custody and retest the path. Retain the designated emergency identity where required; temporary access and permanent recovery capability are different. [09]

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Failure-Specific Paths	Prepare separate recovery for cloud identity, SaaS, on-premises administration, and network devices. Test a repair action, not merely a login screen.
Resilient Custody	Provide authorized access across staff absence and site loss. Protect passwords, security keys, recovery codes, and account-recovery email/phone; avoid a circular vault dependency.
Ready Privilege	Pre-provision the rights and exclusions needed to recover each platform. A role that needs an unavailable approver or PIM service cannot repair that same dependency.
Attribution & Assurance	Maintain account IDs, owners, authorized custodians, and runbooks. Link every use to a named operator and incident; send alerts through a channel usable during the outage.

04 READINESS CHECKS COMPARED

CHECK	SUFFICIENT ALONE?	WHAT IT MISSES
Account Inventory	No	Proves an account exists, not that its credential, role, exception, or recovery method still works.
Credential Inspection	No	Finds missing keys and stale custody records, but does not prove authentication or authorization.
Successful Sign-In	No	An authenticated account may lack the right to repair the failed control or reach the required resource.
Administrative Test	No	Proves one action works; it may still depend on the primary IdP, vault, workstation, or network.
Full Recovery Drill	No	Strongest evidence for the tested scenario. Measure retrieval, repair, alert delivery, and cleanup; untested failures remain unknown.

BREAK-GLASS ACCOUNTS.

PREPARE · RECOVER · VERIFY

05

PROGRAM OPERATIONS

Test the whole chain.

Drill loss of federation, normal MFA, PAM/PIM, a custodian, a site, and the primary network as applicable. Use safe repair actions; record time to usable privileged access and restoration.

Alert on use and change.

Monitor successful and failed sign-ins, credential enrollment, role changes, policy exclusions, and recovery-contact changes. Investigate unplanned activity; preserve account IDs even if names change. [05]

Prevent silent decay.

Check lockout, expiry, dormant-account cleanup, usable keys, and custody after staff or policy changes. Microsoft specifies validation at least every 90 days; apply platform-specific schedules. [01]

Verify the evidence path.

Confirm a human receives the alert and can reach the logs during the simulated outage. Protect log export and retain a local incident record if the central service is unavailable.

06

CONTROL MAPPING

MICROSOFT ENTRA

Use at least two cloud-only .onmicrosoft.com accounts with permanent active Global Administrator assignment. Exclude them from sign-in-restricting Conditional Access policies; protect them with phishing-resistant authentication. [01]

AWS ACCESS

Direct IAM federation bypasses IAM Identity Center, but still needs the external IdP and IAM data plane. Prepare a different path for IdP failure. Keep root access for root-required recovery tasks; no root access keys. [03] [06]

GOOGLE CLOUD

Maintain emergency Cloud Identity/Workspace super admins exempt from SSO. Use multiple FIDO security keys, protected physical custody, and tested access-policy exceptions. Validate the cloud resource permissions needed for the repair. [04]

LOCAL & APPLIANCE

Prepare supported local or console recovery when central authentication fails. Secure physical or out-of-band access; verify platform-specific recovery secrets and privileges without relying on the failed directory.

07

WHAT THIS DOES NOT SOLVE

Provider or Network Loss

A valid identity cannot repair an unavailable provider control plane or missing connectivity. **Service continuity needs separate plans.**

Compromised Admin Device

Malware can steal an authenticated session or misuse real privilege. **Use a trusted recovery workstation.**

Custodian Misuse

Powerful credentials remain attractive to insiders and attackers. **Custody, attribution, and independent review still matter.**

Persistent Attack Changes

Closing a session does not remove attacker-created keys, users, or grants. **Investigate the full scope of compromise.**

08

MYTHS VS. REALITY

MYTH "Break-glass accounts must have MFA disabled."	REALITY Use resilient strong authentication. Microsoft mandatory MFA also applies to emergency accounts accessing covered services. [02]
MYTH "A spare global admin is enough."	REALITY If it shares the failed dependencies, it may also fail. Exercise the complete recovery path.
MYTH "Store everything in the usual SSO vault."	REALITY A vault behind the failed sign-in path creates a loop. Provide protected, independently reachable custody. [06]
MYTH "Every emergency role must be eligible in PIM."	REALITY Activation can itself fail. Entra emergency Global Administrator assignments are permanent active. [01]
MYTH "Always disable the recovery account after use."	REALITY Cleanup follows the platform. Remove temporary access; preserve the tested recovery path.

09

SPEAK THE PROGRAM — KEY TERMS

BREAK-GLASS

A controlled emergency access path used to **restore privileged administration** when normal access fails.

SHARED FAILURE

A single dependency that disables both the ordinary and emergency paths, such as **one IdP or vault**.

CREDENTIAL CUSTODY

The controlled storage, retrieval, return, and renewal of **secrets and authenticators**.

DUAL CONTROL

Two authorized people participate in release or approval; **staff absence must be covered** by the recovery design.

STANDING VS. JIT

Standing privilege is already assigned; **just-in-time** privilege needs activation before use.

RECOVERY DRILL

An exercise proving credential retrieval, authentication, repair authority, **alerting, and cleanup** under a defined failure.