

EMERGENCY BREAK-GLASS & ACCOUNT LOCKOUT

This operational card contains references and procedures only. Never write live passwords, private keys, or recovery secrets on this document.

1. INCIDENT QUALIFICATION: IS THIS A GENUINE BREAK-GLASS EVENT?

- ☐ **Total Administrative Lockout:** All regular tenant/domain administrators are locked out or compromised.
- ☐ **Key Person Catastrophic Absence:** The sole administrator is unreachable and operations face immediate stoppage.
- ☐ **MFA Destruction / Total Factor Loss:** Primary MFA hardware tokens, phones, or authenticators are destroyed/lost.

ABORT CONDITION: Emergency access is **strictly prohibited** for routine tasks, skipping approval delays, or bypassing HR/legal oversight during employee disputes.

2. TWO-PERSON EMERGENCY AUTHORITY & CUSTODY PROTOCOL

Role	Authorized Name & Title	Phone / Emergency Contact	Mandatory Responsibility
Decision-Maker 1			Declares qualifying IT emergency
Decision-Maker 2			Confirms two-person approval
Package Custodian			Holds safe key / sealed custody
Authorized Operator			Executes approved changes only

Policy Rule: Package unsealing requires concurrence from at least two authorized company officers.

3. CONTROLLED EMERGENCY MATERIAL REFERENCES (LAYER 3)

Sealed Recovery Package Reference: RP-_____ • **Status:** Sealed ☐ Opened ☐

Physical Custody Location: _____ (e.g., Safe Room 104)

Emergency Non-Secret Identity: emergency-admin@_____

IT Emergency Binder Reference: Primary Binder Location: _____ (Tab 5)

TECHNICAL EXECUTION & POST-INCIDENT DISPOSITION

ALWAYS MAINTAIN AN AUDIT LOG ENTRY FOR EVERY EMERGENCY STEP

4. STEP-BY-STEP RUNBOOK: BREAKING THE GLASS

1. **Log Opening:** Open an incident log immediately. Record timestamp, declared reason, and all people present.
2. **Inspect & Unseal:** Verify that the security seal on Package RP-_____ is intact. Break seal in the presence of the Custodian.
3. **Authenticate:** Use the dedicated break-glass account. *Alert monitoring teams that legitimate emergency access is in progress.*
4. **Minimal Intervention (Strict Rule):** Do not alter production configurations or perform general maintenance. Restore primary administrator recovery paths only (e.g., reset factor for named admin, create temporary named role).
5. **Sign Out:** Immediately terminate the emergency session across all active endpoints and invalidate session tokens.

5. POST-USE MANDATORY DISPOSITION: RETURNING TO CONTROL

An emergency access state must never be left unsealed or unrotated after an event.

- ☐ **Session Audit Export:** Retrieve provider activity/audit logs and store with the executive record.
- ☐ **Rotate Working Secrets:** Immediately generate a new password and revoke old sessions for the break-glass account.
- ☐ **Re-Key Authenticators:** Replace used one-time recovery codes. Validate physical FIDO2/YubiKey integrity.
- ☐ **Re-Seal Package:** Place fresh materials into a new tamper-evident envelope (RP-_____), sign across seal, record date, and return to safe.
- ☐ **Update Binder Records:** Complete *R13 Binder Change Log* and re-verify *W09* status.

6. EMERGENCY ESCALATION CONTACTS (IF BREAK-GLASS FAILS)

Provider / Support Entity	Routing Identifier / Account Reference	Emergency Phone
Managed Service Provider (MSP)	Customer ID:	Tel:
Identity / Cloud Platform Support	Tenant / Organization ID:	Portal / Tel:
Internet Service Provider (ISP)	Circuit ID / Account:	NOC Tel: