M365 Breakglass Immaturity Model

GitHub.com/KuShuSec v1

🔥 **Fire Hazard**	Used for daily operations
	No MFA enforced
	Password never rotated
	Account exempt from logging
	Alerts suppressed or ignored
	Used from unmanaged or insecure devices
	Password reused anywhere else in the tenant or on-prem AD
	Sign-ins allowed from any country and any IP range instead of a privileged access workstation (PAW)
	Global Administrator kept eligible in PIM rather than permanent (breakglass must bypass PIM)
	Only one breakglass account exists, so any lockout of that identity is catastrophic
🔑 **Shared Secrets**	Account shared between multiple people
	Password stored in plaintext or password manager
	No usage audit trail
	Used for routine mailbox or SharePoint tasks
	No individual accountability or auditability
	Used for Logic Apps, Power Automate, or integration auth
	Credential copies emailed, pasted in chat, or sitting in ticket history
	Stored in DevOps variable groups that a broad set of engineers can read
	Injected by automation into containers or function apps without secret-rotation workflow
	No quarterly attestation forcing each individual to re-confirm "I still know this secret"
	Account federated to on-prem IdP, so if ADFS is down the secret is useless
🕳️ **Hidden Traps**	Credentials embedded in scripts or pipelines
	Breakglass excluded from Conditional Access as workaround
	Cloud-only account with no backup recovery route
	Licensed for all services, increasing attack surface
	Risk-based policies include the account, meaning a high-risk sign-in might be blocked during an actual crisis
	Alternate email and phone set to an ex-employee who is now unreachable
	Account subject to automated cleanup because it has not signed in within the last X days
🙈 **We Don’t Talk About Breakglass**	No documentation or ownership
	Never tested
	No out-of-band recovery plan
	Relying on 'we’ll just reset it'
📉 **Governance**	Runbook rests in a SharePoint site that itself requires normal SSO to open
	No dual-administrator approval recorded when the password envelope is opened
	Recovery exercise never scheduled after tenant migrations or CA revisions
	Owner left the company; their replacement was never assigned in Entra ID
	Incident-response team unaware of the existence of the account until an outage happens
	Post-use review does not revoke the password, leaving an unknown number of copies in circulation