

Quarterly access review — Q3 2026

doc id	RECORD-ACCESS-REVIEW-Q3-2026
version	1
status	record
owner	Olaf Jacobson

Reviewed 2026-09-09 by Olaf Jacobson (Information Security Manager). First review under ISMS-DOC-A05-18-1. Access enumerated directly from the AWS IAM and GitHub APIs rather than from a maintained list, so this is the actual state, not the intended one.

1. GitHub — organisation SoonHQ

Member	Role before	Decision	Role after
OlafJacobson	admin	Keep — CEO / ISM	admin
picaulegend (Thomas Picauly)	member	Promote — CTO had less access than his role requires	admin
A13SSANDRO (Alessandro Cardinali)	admin	Keep — CPO	admin
Melv (Melvin Jacobson)	admin	Keep — see §4, break-glass	admin
CybearSquad (outside collaborator)	—	Keep — external ISMS consultant	outside collaborator

Two-factor authentication is enforced organisation-wide (2026-09-08) and **no member or outside collaborator lacks it**.

2. AWS — IAM Identity Center

Permission sets: SoonDevDatabaseAccess, SoonInfraPlan, SoonInfraApply, PowerUserAccess.

Identities: Olaf, Thomas, Melvin (plus two +udev2 test identities — **action: confirm whether these are still needed**).

3. AWS — legacy IAM users

User	Console	MFA	Privilege	Decision
Olaf	yes	1	Admins (AdministratorAccess)	Keep
Thomas	yes	0	Admins (AdministratorAccess)	Enable MFA immediately — see §5
Alessandro	yes	1	Billing, evidence-capture	Keep
Melvin	yes	2	Admins (AdministratorAccess)	Keep as break-glass — §4
SoonDev0	yes	0	SoonDevs (AWSLambda_FullAccess)	Shared account — open, §6
Auditor	no	0	ReadOnlyUsers	Identify owner and purpose — open

4. Melvin Jacobson — deliberate retention

Melvin holds no operating role (ISMS-DOC-05-2 v0.3). His administrative access is **retained deliberately** as a break-glass measure: he is a founder and shareholder, has the technical background, is already vetted, and is the continuity plan if Olaf or Thomas becomes unavailable. Retaining him materially improves the bus factor for a company whose production estate is otherwise administered by two people.

This is an accepted risk, not an oversight. Conditions attached:

- Access is for **emergency continuity**, not routine work.
- MFA is present (2 devices) and must remain.
- **His long-lived access key (created 2018-04-24, 3,060 days old) is a separate matter from console break-glass access and should be removed** — a continuity account does not need programmatic credentials, and an eight-year-old key is the weakest credential in the estate. Decision pending.
- Reviewed again next quarter.

5. Findings requiring action

#	Finding	Severity	Owner	Status
1	Thomas holds AdministratorAccess with console login and no MFA device. Contradicts the Access Control Policy and the published DPA (Annex II: "protected by multi-factor authentication")	High	Thomas	Open — steps issued 2026-09-09
2	Thomas was <code>member</code> on GitHub while less operationally involved people were admins	Medium	Olaf	Closed — promoted to admin
3	SoonDev0 shared account: console login, no MFA, <code>AWSLambda_FullAccess</code>	High	Thomas	Open
4	Unused access key on <code>SoonDev0</code> (created 2022-08-28, never used)	Medium	Olaf	Closed — deactivated and deleted 2026-09-09
5	Long-lived access keys: <code>serverless</code> (3,068d), <code>SES-Key</code> (3,052d), <code>Melvin</code> (3,060d), <code>Terraform-Cloud</code> (1,673d), <code>Thomas</code> (1,689d and 467d)	Medium	Thomas	Open — rotate those in use, remove those not
6	<code>eb-deployer</code> key last used against Elastic Beanstalk; the platform runs on ECS	Low	Thomas	Open — likely removable
7	<code>Auditor</code> IAM user with an active key that accessed RDS; owner and purpose unrecorded	Medium	Olaf	Open
8	Two <code>+udev2</code> Identity Center identities of unclear purpose	Low	Thomas	Open

6. Actions taken during this review

- Thomas promoted to GitHub organisation admin.
- `SoonDev0` access key `AKIA2Z42KZFEWR4XNP70` deactivated, then deleted (2026-09-09).

7. Next review

Q4 2026. The register of long-lived access keys in §5 is the main carry-over: the target is that no human user holds a static access key, with programmatic access moving to IAM roles and short-lived credentials.

Rendered from SoonHQ/isms — ../../../../private/tmp/claude-501/-Users-olafjacobson-s-isms--claude-worktrees-iso-soc2-evidence-system-3febee/e3e18e8e-8a07-47cd-99b6-574311482138/scratchpad/access-review-q3-2026.md — source SHA-256 b07ca54d3da5561ada6bb9f5e1b75b27ccee555f061a9cbb80c7c05276a4b6a7