

Rules for secure accounts

Editable template for employees and IT. Agree how accounts are protected, recovered and closed. Adapt it to your systems, responsibilities and internal rules before introduction.

Organisation / scope: _____

Owner / approved on / next review: _____

Use individual accounts

Do not share personal accounts. Limit permissions to the task. Keep administrative accounts separate from everyday work.

Manage passwords securely

Use a different long password for each service, generated and stored in the approved password manager. Protect the master password and recovery arrangements appropriately.

Set up suitable MFA

Work with IT to enable strong multi-factor authentication. Where supported, prefer phishing-resistant options such as appropriately configured FIDO2 passkeys or security keys with a PIN or biometrics.

Check sign-in requests carefully

Approve only requests you initiated that match your own sign-in. Reject and report unexpected requests. Do not give callers your password, one-time code or recovery code.

Prepare recovery in advance

Agree a backup factor and authorised recovery process. Store codes securely under internal rules, not solely behind the locked account. Never enter codes in this template.

Report changes and concerns

Promptly report lost devices, suspicious sign-ins and permissions no longer needed. If compromise is suspected, IT also coordinates review of sessions, factors and application access.

Internal contacts

Approved password manager / internal guide: _____

IT contact / fallback contact when locked out: _____

Location of recovery instructions without codes: _____

Account recovery checklist

Use the agreed process only for your own accounts or accounts you are explicitly authorised to administer. Involve the responsible IT team; this template does not authorise account takeover.

Affected service / internal case / time: _____

Reachable contact / verified by: _____

Identify the situation

Lost device, broken factor or suspicious sign-in? If compromise is suspected, use the internal incident route immediately; changing the password alone may not be enough.

Use a known contact

Contact IT through the recorded number or known portal. Do not seek help through unverified search ads, unfamiliar callback numbers or unexpected links.

Let IT verify identity

Follow the agreed identity-checking procedure with IT. Urgency does not replace verification. Do not disclose MFA codes to callers.

Use an approved fallback

Use a backup factor or secure recovery procedure as authorised. Have lost factors revoked and new factors registered under controlled conditions.

Review other access if compromise is suspected

IT checks active sessions, tokens, application grants, recovery details and mailbox rules, among other relevant items. Block or revoke affected access as appropriate.

Record completion

Test contact routes and sign-in, update the fallback and document actions in the internal case. Do not copy secrets into the record.

Actions / owner / completed on: _____

Sign-in test result / next review: _____

Grant change and revoke access

For joining, changing roles and leaving. HR, the business owner and IT agree approval, implementation and review dates. Add rows for additional services.

Person or internal reference / role: _____

Reason / effective from / approved by: _____

Service or account	Required access and action	Completion and evidence
_____ _____	_____ _____	_____ _____
_____ _____	_____ _____	_____ _____
_____ _____	_____ _____	_____ _____
_____ _____	_____ _____	_____ _____

When joining or changing roles

Verify identity and approval, grant only necessary access and prepare MFA and recovery. Explicitly remove old permissions after role changes. Record expiry and the next review; approve administrative privileges separately.

When leaving

At the approved time, disable accounts and remote access, revoke sessions and tokens and review MFA factors. Include services outside the central login. Check devices, keys and shared secrets; rotate affected shared secrets. Transfer data and responsibilities under internal rules. Address deletion and retention separately.

Completion checked by / date / open issues: _____

Use and sources

Original Paragamix GmbH templates. Free to use internally, adapt and share with clients. A source link is welcome but not required. Not a complete access audit or confirmation of compliance. Never record passwords, tokens or recovery codes.

[NCSC Identity and access](#) | [NCSC MFA](#) | [NCSC Password managers](#)

[Current version and practice cases](#)