Passwords, MFA and access policy

Organisation	Version	Approved by	Approval date	Next review
[Organisation name]	[1.0]	[name, role]	[dd-mm-yyyy]	[dd-mm-yyyy, at least yearly]

How to use this template (delete this box before issuing)

- Replace every [bracket] with your own facts. Where you see **Choose:** keep one option and delete the others.
- The grey "Why this rule" boxes explain the reasoning. Delete them before you issue the policy, or keep them: staff follow rules better when they know why.
- Scale it to your size. A five-person firm can fill in one name for several roles. Delete rules that do not apply, and mark them "Not applicable" in 09-Implementation-tracker.xlsx.
- This is a template, not legal advice. It does not guarantee compliance with any law or standard. Check employment and privacy rules in your own country before you issue it.

Sample — lerider.

1. Purpose

A stolen or guessed password should never be enough to get into our systems, and people should have access only to what they need for their work. This policy sets the rules for passwords, multi-factor authentication (MFA) and access rights at [Organisation].

2. Passwords

- Length: at least **[14] characters** for accounts that are not protected by MFA, and at least **[12]** where MFA is on. A passphrase of four or more random words is a good way to get there.
- No forced complexity rules or maximum length, and no forced periodic changes. Change a password when there is a reason: suspected compromise, a leak, or when someone who knew it leaves.
- Every account has its own password. Never reuse a work password anywhere else, and never reuse a private password for work.
- Use the company password manager: **[name of tool]**. **Choose:** [Its use is required for all work accounts.] / [Its use is required for shared and administrator accounts and recommended for all others.]
- Never write passwords on notes, in documents or in e-mail or chat. Shared passwords are shared through the password manager only.
- Where a system can check new passwords against lists of known leaked passwords, this check is switched on.

Why this rule

European cybersecurity agencies have moved away from complex passwords that must change every 90 days. Germany's BSI, for example, says passwords should only have to be changed for a valid reason, and the Dutch NCSC advises long passwords without a forced maximum. Forced changes lead to predictable patterns (Summer2026!, Autumn2026!). Length, uniqueness and MFA protect far better.

Sample — the full bundle: lerider.com/shop/iso27001-policy-starter-bundle/

3. Multi-factor authentication (MFA)

MFA is required for at least:

- e-mail and the office suite (for example Microsoft 365 or Google Workspace);
- remote access to our network or systems (VPN, remote desktop);
- all administrator accounts, including those of our IT provider;
- online banking, payroll and accounting systems;
- cloud services that hold Confidential information or personal data: [list].

Approved methods, in order of preference: [passkey or hardware security key] → [authenticator app with number matching] → [text message (SMS), only where nothing else is offered].

- Never approve an MFA prompt you did not start yourself. Report it to [name / contact] at once: it means someone has your password.

> **Why this rule**
>
> Most account takeovers start with a phished or reused password. MFA stops the large majority of these, which is why NIS2 names it explicitly in art. 21(2)(j) and why customers ask about it in almost every security questionnaire.

4. Access rights

- Access is granted per role ("need to know"), not "everyone sees everything". [Role] approves access to Confidential information.
- New staff, role changes and leavers follow 07-Onboarding-offboarding-checklist.xlsx. Accounts of leavers are disabled on their last working day at the latest.
- Administrator rights are given only to people who need them. They use a separate admin account for admin work, and a normal account for e-mail and browsing.
- Shared accounts are avoided. Where one is unavoidable, it has a named owner, it is stored in the password manager, and its password is changed when someone with access leaves.
- **Choose:** [Every quarter] / [Every six months], [role] checks who has access to [key systems] and removes access that is no longer needed. The check is logged in 09-Implementation-tracker.xlsx.
- Default passwords on new equipment (routers, printers, cameras, Wi-Fi access points, software) are changed before the equipment is used.

> **Why this rule**
>
> An account that stays active after someone leaves is one of the most common gaps in small organisations, and it is invisible until it is misused. A short periodic review finds it.

5. When a password or account may be compromised

If you think a password, MFA method or account is compromised:

- change the password at once, from a device you trust;
- report it to [name / contact], who signs out all active sessions and checks for changed settings such as new mail-forwarding rules;

Sample — the full bundle: lerider.com/shop/iso27001-policy-starter-bundle/

- follow 05-Incident-response-plan if data may have been accessed.

6. Approval and review

Owner of this policy: [name, role]. The owner keeps it up to date and answers staff questions about it.

Review: at least once a year, and after any serious incident, a major change in systems or a new legal requirement. Record the review in 09-Implementation-tracker.xlsx (tab "Review calendar").

Approved by (name, role)	Signature	Date
[ ]		[dd-mm-yyyy]

Where this policy helps

Useful when a customer, auditor or insurer asks which of your documents covers a topic. References are to article numbers and control numbers only; the text of the standards is not reproduced.

Framework	Reference	Note
GDPR (EU) 2016/679	art. 32(1)(b)	Ongoing confidentiality of systems processing personal data
NIS2 (EU) 2022/2555	art. 21(2)(i), (j)	Access control policies; MFA. Only relevant if you are in scope, or a customer asks.
ISO/IEC 27001:2022 Annex A	5.15, 5.16, 5.17, 5.18, 8.2, 8.5	Who may get in and how: accounts, passwords and other login secrets, access rights, admin accounts, safe sign-in
ENISA guide for SMEs	step 5	Secure access to systems

Sample — lerider.com

Sample — the full bundle: lerider.com/shop/iso27001-policy-starter-bundle/

IT security at [Organisation]: the 12 rules we all follow

One page for everyone. The full policies are at [location]. Questions: [name / contact].

1	**Your account is yours.** Never share passwords or MFA codes, not even with colleagues or "IT support" on the phone.
2	**Long and unique passwords.** At least [14] characters, a different one for every account, kept in [password manager].
3	**MFA everywhere it is offered.** Never approve a sign-in prompt you did not start. Report it.
4	**Lock your screen** when you walk away, also at home.
5	**Updates are not optional.** Install them within [3] working days.
6	**Check payment changes by phone.** New bank details or an urgent payment request: call a number you already know.
7	**Think before you click.** Unexpected link, attachment or urgent request? Ask first.
8	**Confidential stays confidential.** Personal data, contracts and finances go only to people who need them, through [approved channels].
9	**Approved tools only.** No unapproved apps, cloud storage or AI tools for company information.
10	**Work files in [company storage],** not only on your laptop or a USB stick.
11	**Report lost devices within [1 hour],** day or night: [phone].
12	**Report mistakes at once.** Clicked something, sent something to the wrong person? Tell [name] now. Speed matters, blame does not.

Report security problems to

[Name] · [phone, also out of hours] · [e-mail]

Sample — lerider.com

Sample — the full bundle: lerider.com/shop/iso27001-policy-starter-bundle/

Staff acknowledgement

I have received and read the following documents, and I know where to find them and whom to ask:

☐ IT security: the 12 rules we all follow (this page)

☐ 01 Acceptable use policy

☐ 02 Passwords, MFA and access policy

☐ 03 Remote work and own devices policy

☐ [05 Incident response plan: the parts that apply to me]

☐ [other:]

I will report security incidents, lost devices and mistakes as described.

Name	Role	Date	Signature

Keep the signed form, or a confirmation by e-mail or in your HR system, in the staff file. Repeat it when a policy changes in a material way. Record the date in 07-Onboarding-offboarding-checklist.xlsx.

Sample — lerider.com

Sample — the full bundle: lerider.com/shop/iso27001-policy-starter-bundle/