Password & Access Policy — Template

Short on purpose — policies people read beat policies that impress auditors.

Organisation: _____ · **Approved by:** _____ ·

Review: _____

1. Passphrases, not passwords

- Use a **passphrase of four or more random words** (e.g. `paddock-lantern-cricket-mango`) or a password manager's generated password.
- **Never reuse** a password across sites. One leak shouldn't open every door.
- No sticky notes, no shared spreadsheets of passwords.

2. Use the password manager

- We use: _____ . Every staff member gets an account.
- Store all work credentials in it. Let it generate and fill passwords.
- Your master passphrase is the one passphrase you memorise. Make it long. Never share it.

3. Multi-factor authentication (MFA)

- MFA is **mandatory** on email, banking, admin accounts and _____ .
- Use an authenticator app where possible (stronger than SMS).
- **Never share an MFA code with anyone** — no legitimate person will ever ask. Anyone asking is a scammer, every time.

4. Sharing and leaving

- Share access via the password manager's sharing feature — never by email or chat.
- When someone leaves: disable their accounts within _____ , rotate any shared credentials they had.

5. Admin accounts

- Admin rights only for people who need them, reviewed _____ .
- Admins use separate everyday and admin accounts.

6. If a password may be exposed

Change it immediately, tell _____ , and check for unfamiliar logins or email rules. **No blame for reporting — ever.**