



Team Security and Acceptable Use Policy

Date _____

1. Who this applies to

This policy applies to everyone who has access to **PandaDev**'s systems: staff, sub-admins, admins and contractors ("the Team Member"). Signing it confirms the Team Member has read it and will follow it.

2. Accounts and passwords

- Turn on two-factor authentication on every Studio account.
- Use a password manager and a different strong password for each account.
- Never share an account, a password or a sign-in code, even with another team member.

3. Devices

- Keep devices up to date, locked with a PIN or password, and with disk encryption turned on.
- Do not work on Studio or client systems from shared or public computers.
- Report a lost or stolen device to the Studio within 24 hours.

4. Client data

- Use client data only for that client's work, and only inside the Studio's approved tools.
- Do not copy client data to personal email, personal storage or unapproved apps, including AI tools.
- Never put real client data into test systems, screenshots or demos unless the client agreed.

5. Code and keys

- Never put passwords, API keys or secrets in code, tickets, chat or email.
- Work through the Studio's repositories and review process; do not push straight to live systems unless your role allows it.

6. Reporting

Report a suspected breach, phishing email or mistake with data to support@pandadevhub.com straight away. Reporting quickly is always the right thing to do; nobody is blamed for an honest report.

7. Checks and changes

The Studio may review access logs to keep systems safe and may update this policy, telling the Team Member about any change. Breaking this policy can lead to access being removed and the engagement ending.

Signatures

TEAM MEMBER

Name:

Date:

FOR THE STUDIO

Name:

Date: