

Access Security and Authentication

Responsibilities for protecting accounts and authorizing operations.

Key points for reference

- Use individual accounts and two-factor authentication.
- Never send passwords in public forms.
- Account recovery requires proportionate verification.

Reference summary. The complete clauses below prevail.

1. Responsibilities and scope

This covers customer accounts, panels, administrative access, integrations and authorized users. Zovvi protects managed components; customers protect their devices, applications and permissions. Incidents are assessed by cause and duties without automatically assigning all liability to the account holder.

2. Passwords, factors and devices

Use long unique passwords, a trusted manager and available two-factor authentication. Keep recovery material separate. Arbitrary periodic rotation does not substitute for security; change passwords after compromise or justified advice.

Sensitive actions may require disclosed additional confirmation or a second factor. Update and lock devices. Support does not request passwords or one-time codes through unsolicited contact.

3. Teams, delegation and privileges

Prefer individual access, least privilege and prompt revocation when relationships end. Identify who may administer, purchase or delete services. Use available delegation or limited authorization rather than sharing primary credentials with agencies.

Sensitive changes require authority checks. Knowing a domain or being copied on email does not prove ownership. Access disputes require evidence and protection for all parties.

4. Keys, integrations and technical access

Tokens and keys require minimal scope, protected storage and rotation after exposure. Do not publish them in code, URLs, screenshots or public tickets. Use temporary access through the indicated secure channel for support or migration and revoke it afterward.

Zovvi technical access must be necessary, limited and confidential. Diagnostics do not authorize unrelated data use. Overwrites or availability-impacting changes require appropriate scope and authorization.

5. Recovery and suspected incidents

Contact official support about lost access, suspicious logins or scams. Provide service, time and facts without secrets. Recovery may require proportionate ownership checks and protected documents; a payment receipt alone does not transfer control.

Concrete risks may require session termination, token revocation or component isolation, with reasons and next steps communicated when feasible. Measures must not improperly obstruct review or rights. Incident data follows the Privacy Policy.

6. Applications and review

Update CMS software, plugins and dependencies, remove unused access and keep independent backups. SSL protects transport but does not guarantee vulnerability-free software or legitimate messages. Additional requirements must be proportionate, explained and compatible with the purchased service. Request review of excessive checks or restrictions.

