Grow Us Today

Websites That Help Your Business Grow

Security

Last Updated: 15 May 2026 | Contact: support@growustoday.com

1. Introduction

This Security Policy outlines the technical and organisational measures used by Grow Us Today to help protect our website, project enquiry systems, admin dashboard, backend infrastructure, and related services against unauthorised access, misuse, loss, disclosure, or disruption.

While no online system can be guaranteed completely secure, we aim to apply reasonable and proportionate safeguards appropriate to the nature of the services we provide.

2. Scope

This policy applies to:

- The Grow Us Today public website
- Project enquiry and contact forms
- Internal admin dashboard systems
- Backend infrastructure and APIs
- Authentication systems
- File and document storage systems
- Session and audit logging systems
- Connected third-party infrastructure providers

This policy also applies to authorised staff, contractors, administrators, and approved users with access to internal systems or dashboard environments.

3. Systems & Data Covered

Our systems may process business and personal information including:

- Names
- Business details
- Email addresses
- Phone numbers
- Project information
- IP addresses
- Authentication and session data
- Uploaded documents
- Activity and audit records
- Device and login metadata

The admin dashboard may also process role-based account information, client project data, session history, document references, and operational records necessary for service management.

4. Access Control & Authentication

Access to internal systems and dashboard functionality is restricted to authorised users only.

Security measures may include:

- Firebase Authentication
- Verified authentication tokens
- Role-based access controls
- Session validation
- Account status enforcement
- Password protection requirements
- Device and session monitoring
- Refresh token revocation where appropriate

Administrative privileges are limited according to operational necessity.

Higher-risk actions, including user-management functions and privileged account changes, may be restricted to elevated administrator roles.

Where accounts are deleted or disabled, associated sessions and authentication tokens may also be revoked.

Users are responsible for:

- Keeping passwords confidential
- Using strong and unique passwords
- Avoiding password reuse across services
- Reporting suspected unauthorised access promptly

5. Application & Platform Security

We implement security controls designed to reduce abuse, spam, unauthorised access, and malicious activity.

These measures may include:

- Input validation
- Required field validation
- Email and phone validation
- CSRF and abuse protection mechanisms
- Google reCAPTCHA verification
- Honeypot detection
- Rate limiting and request throttling
- Session management controls
- Activity monitoring and audit logging
- Secure backend API validation

Public-facing endpoints may be restricted to approved request methods and monitored for suspicious activity.

Security logs and operational activity records may be retained for monitoring, investigation, and incident response purposes.

6. Session Monitoring & Audit Logging

The admin dashboard may maintain session and audit records to support operational security and account protection.

Depending on the system feature involved, logs may include:

- Login timestamps
- Device information
- Device labels
- IP addresses
- Approximate geographic information
- Session status
- User actions
- Administrative events

Sessions may be remotely invalidated where supported.

Operational logs and activity records are periodically reviewed and retained only for as long as reasonably necessary.

7. File & Document Security

Uploaded documentation and stored files are protected through access restrictions and controlled delivery methods.

Security measures may include:

- Restricted upload permissions
- File-type validation
- Controlled storage environments
- Signed or expiring access links
- Role-based document permissions
- Access logging and monitoring

Where supported, sensitive files are not exposed through permanent public URLs.

Only authorised users should be able to upload, view, rename, delete, or download protected documentation.

8. Infrastructure & Secret Management

Sensitive credentials and infrastructure secrets should be handled securely and never intentionally exposed publicly.

Security practices may include:

- Environment variable configuration
- Managed secret storage
- Restricted administrative access
- Credential rotation procedures
- Secure deployment practices
- Separation of client-side and server-side credentials

Private keys, authentication secrets, API credentials, email service keys, and similar sensitive values should not be stored within public repositories or exposed client-side unless explicitly designed for public use.

9. Third-Party Providers

Our systems may rely on third-party infrastructure and service providers including:

- Google Firebase
- Google reCAPTCHA
- Resend
- Tawk.to
- Hosting and DNS providers
- Domain registrars
- Analytics and communication providers

These providers operate under their own operational, security, and privacy policies.

While we aim to select reputable providers, we cannot guarantee uninterrupted service availability or security controls outside our direct operational control.

10. Operational Security

To help maintain platform security, we aim to:

- Keep software dependencies reasonably up to date
- Remove unnecessary or outdated deployment files
- Review third-party integrations before deployment
- Restrict administrative access
- Monitor for suspicious activity where practical

- Apply security updates and configuration changes where appropriate

Development, staging, and production environments should be appropriately separated where feasible.

11. Incident Response

If a suspected security incident or personal data breach occurs, we may take actions including:

- Disabling affected accounts or sessions
- Revoking authentication tokens
- Rotating exposed credentials or secrets
- Restricting vulnerable systems or endpoints
- Preserving logs and evidence for investigation
- Investigating the nature and impact of the incident

We aim to assess incidents promptly to determine operational, legal, and data protection obligations.

Where required under applicable law, reportable personal data breaches may be disclosed to the Information Commissioner's Office (ICO) and affected individuals within legally required timeframes.

Following an incident, we may review controls, update procedures, and implement additional safeguards where appropriate.

12. User Responsibilities

Users of our systems and dashboard services are expected to:

- Maintain account security
- Avoid sharing credentials
- Use systems lawfully
- Avoid uploading malicious or unlawful content
- Report suspected vulnerabilities or security concerns responsibly

Users must not attempt to bypass security protections, gain unauthorised access, interfere with systems, or disrupt services.

13. Limitations

Although we apply reasonable security measures, no internet-based system, software platform, or transmission method can be guaranteed fully secure or uninterrupted.

Users acknowledge that all online services carry inherent operational and security risks.

14. Policy Review & Updates

This Security Policy may be reviewed and updated periodically to reflect changes in infrastructure, legal obligations, operational practices, or security controls.

The latest version will always be published with the updated revision date shown above.

15. Contact

Questions relating to this Security Policy or responsible security disclosures may be sent to: support@growustoday.com