Support Policy

Effective date: June 18, 2026

This Support Policy explains how Cloud Technology Computing provides technical support for websites, cloud services, applications, AI solutions, managed IT services, and related technology services.

1. How to Request Support

Customers may request support through:

- Email: Jgil20@me.com
- Phone: 1-713-870-9966
- Website contact or consultation form
- Any dedicated support channel identified in the customer's service agreement

Please include the affected service, a description of the problem, screenshots or error messages, when the issue began, and any recent changes that may be relevant.

2. Support Availability

General support requests are reviewed during normal business operations. Response times depend on the customer's service plan, the severity of the issue, available staff, and whether the issue involves a third-party platform.

Emergency, after-hours, holiday, or 24/7 support is available only when included in a written managed-services agreement.

3. Issue Priority

Support requests may be classified as follows:

Critical: A production website, application, cloud environment, or essential business system is unavailable, and no reasonable workaround exists.

High: A major feature is unavailable or significantly impaired, but some business operations remain available.

Normal: A limited feature is affected, a workaround exists, or the request involves configuration, troubleshooting, or maintenance.

Low: A general question, enhancement request, cosmetic issue, content update, or non-urgent change.

Priority classifications may be adjusted after technical review.

4. Response and Resolution

Any stated response time is a target for acknowledging or beginning review of a request. It is not a guaranteed resolution time.

Resolution may depend on:

- Customer access and cooperation
- Hosting-provider availability
- Software vendors and cloud providers
- Domain, DNS, email, or payment processors
- Security investigations
- Third-party APIs and integrations
- The complexity and scope of the problem

Cloud Technology Computing will provide reasonable updates while an active support request is being investigated.

5. Customer Responsibilities

Customers are responsible for:

- Providing accurate information and authorized access
- Maintaining current contact and billing information
- Protecting passwords and administrator credentials
- Following security recommendations
- Maintaining valid third-party subscriptions and licenses
- Reporting suspected security incidents promptly
- Avoiding unauthorized changes while troubleshooting is underway

Delays caused by missing access, incomplete information, unsupported software, or customer-controlled systems may affect response and resolution times.

6. Supported Services

Support applies only to services, systems, applications, and configurations covered by an active agreement or approved project scope.

Additional fees may apply for:

- Work outside the agreed scope
- New features or redesigns
- Data recovery
- Malware remediation
- Emergency work
- Third-party migration
- Unsupported or outdated systems
- Damage caused by unauthorized changes

Approval may be required before billable work begins.

7. Third-Party Services

Some services depend on third parties such as AWS, Microsoft Azure, Google Cloud, IBM Cloud, Hostinger, Cloudflare, Stripe, PayPal, domain registrars, software vendors, and API providers.

Cloud Technology Computing may assist with troubleshooting, but cannot guarantee the availability, performance, policies, security, or response times of third-party services.

8. Backups and Data Recovery

Backups are provided only when included in the customer's service plan or project agreement. Customers should maintain independent copies of important business data.

No backup or recovery system can guarantee that every file or version will be recoverable. Restoration work may be billed separately unless expressly included in the customer's agreement.

9. Security Incidents

Suspected unauthorized access, malware, credential theft, or data exposure should be reported immediately.

Cloud Technology Computing may temporarily restrict access, disable integrations, reset credentials, isolate affected systems, or recommend additional security measures when reasonably necessary to protect systems and data.

10. Policy Changes

This Support Policy may be updated as services, technologies, and business practices change. The updated version will be posted on the website with a revised effective date.

Contact

Cloud Technology Computing
Houston, Texas
Email: Jgil20@me.com
Phone: 1-713-870-9966
Website: https://www.cloudtechnologycomputing.com/