



JUNE '26 INSIGHTS

Accelerated Computing Enterprise is the Indian arm of Cloud Ace Group.

Cloud Ace was established in Japan in 2014 and became the first Managed Service Provider (MSP) for Google Cloud in the country. Cloud Ace have won the Google partner of the year award in 2018 & 2021 as we continued to grow our business to other part of Asia and now we are expanding into Europe, North and South America as well as Africa.

We can help you in digital transformation by modernizing your infrastructure with best in-class cloud-native and cloud advisory services.

Inside This Issue

- Our Mission, Vision & Commitment
- Specialization
- Our Services
- Our Global Collaboration
- **Article**
- **Terms of Services**
- **Team Gathering**

10
Countries

600+
Experts

1000+
Happy Clients

OUR MISSION

Build our work on Honesty.

It is our mission with an unwavering pride that we are always aware of as we work to realize our vision; not just being honest, but “Honesty itself is our work and our service.”

OUR VISION

To contribute to building a world where all people can utilize advanced technology and realize the dreams they have envisioned.

We aspire to build a world where every person in the world can achieve their ambitions through the use of advanced technology. Our vision is to create such a world and help those who want to achieve it.

OUR COMMITMENT

As Google Cloud Partners, we are committed to providing our clients with cutting-edge technologies and exceptional customer service. Our team of experts is trained and certified to help you leverage the full potential of the Google Cloud Platform, from cloud storage and networking to machine learning and artificial intelligence.

SPECIALIZATION

This achievement reflects our continued commitment to delivering exceptional cloud solutions and deep technical expertise on the Google Cloud Platform (GCP). More importantly, it enables us to offer you enhanced support through Google Funding, specifically for any Engineer Support work related to GCP.

What this means for our Clients:

- Access to Google-backed funding to support your cloud engineering initiatives
- Priority support from certified experts across various GCP services
- Improved delivery capabilities and faster time-to-value for your projects
- Recognition that you're working with a trusted, Google-verified partner

We'd love to explore how we can leverage this specialization to add more value to your current or upcoming cloud initiatives. Please let me know a convenient time for a quick call or feel free to reply here — we're excited to help you get started.

Looking forward to continuing our collaboration with even more momentum!



SPECIALIZATION

Infrastructure

Google Cloud

OUR SERVICES



Managed & Consulting Services

Our Managed & Consulting Services Portfolio includes Cloud Infrastructure Services, Cloud Migration Assessment & Planning, Billing & Cost Optimisation, Monitoring, Security, Incident Management and on-going Support Activities.



System Migration, Design, Development & Automation

We provide Application Development, Modernisation Solutions, Cloud Migration Deployment & Optimisation, POCs, Infrastructure Orchestration & Continuous Improvement Activities.



Multi-Cloud, Hybrid Cloud, Backup & Recovery Solutions

If our Customers have Multi-cloud or Hybrid Cloud needs, as Google Cloud Partners, we can help them manage the most Complex Cloud Environments.



AI/ML, Gen AI, Data Engineering, Reporting & IoT Services:

We specialise in providing AI/ML and GenAI Solutions. We can also help our Customers with Data Warehousing, Data Analytics, Dashboarding & Reporting Solutions on top of Google Cloud's Data Services.



Training & Adaptation

Our Certified Professional Google Certified Trainers can help you in Training to ensure that your Team & your Customers are Knowledgeable in GCP & GWS Best Practices, which can inspire Client Confidence.



Google Workspace

We provide Google Workspace Deployment & Migration Business Solutions for setting up Gmail, Google Drive, Google Calendar and other Productivity tools.

OUR GLOBAL COLLABORATION

Expanding Our Global Collaboration to Strengthen Google Cloud Project Delivery in India

At Cloud Ace, we take pride in being one of the leading Google Cloud Partners globally, with a strong footprint across multiple markets. As a Japanese cloud technology company, our commitment to delivering high-quality cloud solutions has always been at the heart of everything we do.

In India, the demand for Google Cloud SI&C (System Integration & Consulting) projects continues to grow rapidly. To ensure we meet and exceed client expectations while maintaining the highest standards of delivery, we are now actively collaborating with our global divisions—including teams from Japan, Vietnam, Hong Kong, and Indonesia.

This strategic collaboration allows us to leverage engineering talent and technical expertise across borders, enhancing our delivery capabilities and ensuring timely execution of projects in India. By aligning with our overseas teams, we aim to bring the best of global knowledge and experience to our local engagements.

This is a significant step forward in our mission to provide reliable, scalable, and future-ready Google Cloud solutions to enterprises in India.

Together, across borders, we continue to build smarter with the cloud.

Cloud Security Spotlight

Defending Your Infrastructure Against GenAI Billing Exploits

As Generative AI continues to accelerate how we build and deploy applications, the speed of innovation has introduced a new frontier of cloud security and financial challenges.

At Cloud Ace, we believe that transparency and proactive education are our strongest tools for collective defense. Recently, the cloud ecosystem has witnessed a sharp increase in unauthorized API usage, leading to catastrophic billing anomalies for several organizations.

Recently, one of our customers received a Gemini API bill of approximately INR 1.6 million in a single billing cycle in just a few hours. The customer confirmed this usage was unexpected and likely the result of compromised or unrestricted API keys. We immediately stepped in to help this customer contain the issue and prevent further billing leakage.

Below, we break down the exact technical anatomy of how these incidents occur, the aggressive defensive steps our team took to protect your business, and the architectural blueprint required to secure your AI workloads moving forward

Anatomy of an Exploit

When an incident of this scale occurs, it is almost never due to a breach of Google Cloud's underlying infrastructure. Instead, it stems from a cascading vulnerability involving credential management on local development environments.

1. The Local Exposure

The primary vector for these exploits often begins during the development or testing phase. A developer might inadvertently store an active API key in a local configuration file, an environment variable (.env), or a hardcoded script on their local laptop. If that machine is compromised by localized info-stealing

malware, or if the code is accidentally pushed to a public repository like GitHub, the key is instantly scraped by automated malicious bots

2. The "Unrestricted" Default Trap

By default, newly generated API keys in the Google Cloud Console are set to "Unrestricted." This means the key has the authority to call any enabled service within that specific GCP project. If a key originally meant for a low-cost front-end service (like Google Maps or Firebase) is leaked, it carries those blanket permissions with it.

3. The Latent API Exploitation

The financial damage triggers the moment the Gemini API (Generative Language API) is enabled in that project—even if it is only enabled for an internal proof-of-concept and never deployed to production.

Malicious bots, which continuously test scraped keys against premium AI endpoints, instantly detect that the key now has access to high-performance language models. The attackers then launch massive, automated, high-volume parallel workloads. In the incident referenced above, the automated script managed to execute nearly 8,000,000 requests in a matter of hours, entirely bypassing the organization's actual applications.

Chronology of the Crisis



The Danger of Billing Latency: Disabling a compromised API key does not stop the visible charges immediately. Because cloud billing pipelines process usage data in batches, there is an inherent latency between the moment a resource is consumed and the moment it reflects on your financial dashboard. During this lag, charges will continue to appear to rise even after the attack vector has been severed.

Our Active Defense Protocol: Hands-On Protection

To ensure our customers remain fully insulated from these vulnerabilities, the Cloud Ace India Team didn't just issue a warning—we shifted into an active defense posture. We held mandatory, 1-on-1 emergency technical sessions with our customers to lock down their environments. During these shared screen sessions, we implemented four absolute lines of defense

Enforced Rigid Quota Caps: We overrode the default, high-ceiling Google limits and put strict per day and per-minute quota caps on the Generative Language and Vertex AI APIs. This ensures that even if a key is leaked, the maximum possible financial exposure is capped at a negligible amount.

Applied Hard Restrictions: For teams utilizing Google AI Studio, we removed the "Unrestricted" status. We locked keys down to specific backend server IP addresses or verified HTTP referrers, rendering the keys completely useless if scraped by external bots.

Decommissioned Inactive Vectors: If a customer project had the Gemini API enabled but wasn't actively using it in their live architecture, we guided them to disable the API entirely, shrinking the project's attack surface.

Initiated Vertex AI Migrations: We actively advised moving production workloads to Vertex AI to permanently eliminate the risks associated with static API keys.

The Strategic Shift: Why We Strongly Recommend Vertex AI

If you are building enterprise or high-security applications, the absolute best practice is to stop using API keys altogether. We strongly recommend migrating from Google AI Studio (which relies on static API keys) to Google Cloud Vertex AI

Security Feature	API Keys (Google AI Studio)	Service Accounts (Vertex AI)
Authentication	Static string (AIza . . .)	Short-lived, dynamically generated OAuth tokens
Exposure Risk	High (if embedded in frontend)	Zero (cannot be executed from a client browser)
Access Control	Broad (project level)	Granular (Identity and Access Management / IAM roles)
Network Security	Public internet only	Supports VPC Service Controls for private networking

The 5-Step Security Blueprint

If you must use API keys for legacy systems or rapid prototyping, follow this precise sequence in your Google Cloud Console to lock down your environment and prevent unauthorized billing spikes.

1 Audit and Isolate Projects

Never mix public services with AI workloads

Navigate to **APIs & Services > Enabled APIs & Services**. Ensure that you are not using the same GCP project for public-facing frontend services (like Google Maps or Firebase) and Generative AI. If you are, create a dedicated, isolated project specifically for your Gemini/Vertex AI workloads.

2 Eliminate Unrestricted Keys

Apply API Restrictions

Navigate to **APIs & Services > Credentials**. Look for any API keys with a yellow warning icon indicating they are "Unrestricted." Click the key, scroll to **API restrictions**, choose *Restrict key*, and select **ONLY** the specific APIs that key needs to access.

3 Apply Application and IP Restrictions

Lock down where the key can be used

On the same Credentials page, scroll to **Application restrictions**. Restrict the key's usage to specific known entities. Lock HTTP referrers to your specific website domains, or lock IP addresses to your specific backend server IP addresses.

4 Cap API Quotas

Set mathematical limits on usage

Go to **IAM & Admin > Quotas & System Limits**. Filter by the *Generative Language API* or *Vertex AI API*. Override the default limits and set strict **per-minute** and **per-day** request quotas. Set this limit to just slightly above your expected peak usage.

5 Configure Billing Budgets and Alerts

Catch anomalies within hours

Navigate to **Billing > Budgets & alerts**. Create a new budget for your project and set aggressive threshold alerts at **50%, 70%, 90%, and 100%** of your expected monthly spend. Ensure these alerts are configured to email your cloud administrators immediately.

Partnering for a Secure Cloud Journey

As your cloud and billing partner, Cloud Ace is fully committed to defending your infrastructure and escalating forensic investigations with Google when anomalies occur. However, day-to-day credential hygiene and local machine security remain a vital shared responsibility.

As a billing partner, we are ready to help out to the maximum of our capabilities. However, since we are just a billing partner, we don't have an overview or control over your workload. Please take necessary actions yourselves, or let us know if you need help—we are always happy to help

CAIN THE SERVICES TERMS OF USE

- **Article 1 Purpose**

-
- These Terms of Use apply to users of Google Cloud Platform (hereinafter referred to as “GCP”) provided by Google LLC. (including, but not limited to, Google’s affiliates; hereinafter referred to as “Google”), and to [Accelerated Computing Enterprise Pvt. Ltd. (Cloud Ace India), (hereinafter referred to as “CAIN”). The purpose of these Terms of Use is to establish the terms and conditions for the Services (defined in Article 2).
- If a person or an organization applying for the Services (hereinafter referred to as the “Applicant”) applies to CAIN using the prescribed application or purchase method and CAIN accepts the application, the Applicant and CAIN shall agree that these Terms of Use apply to the Services and these Terms of Use shall constitute the usage contract between the parties.
- The Applicant acknowledges and agrees that these Terms of Use may be provided electronically, including through CAIN’s website, online portals, order forms, electronic acceptance mechanisms, or other digital means. The Applicant’s execution of a Purchase Order, click-through acceptance, use of the Services, or payment of invoices shall constitute acceptance of these Terms of Use.

-
- **Article 2 The Services**

-
- The Services provided by CAIN to the Applicant shall be as follows:
 - Providing GCP usage services with mutually agreed discounts on usage fees.
 - Acting as a payment agency for GCP usage fees in India Rupee.
 - Unless expressly agreed in writing under a separate support, managed services, professional services, or support agreement, CAIN acts solely as a billing reseller and payment management provider for Google Cloud services.
- CA shall not be responsible or liable for:
 - any workload failures, application failures, configuration issues, security incidents, downtime, data loss, performance degradation, or operational issues occurring within the Applicant’s environment;
 - any interruption, degradation, suspension, malfunction, or failure of Google Cloud Platform or related Google services;
 - any technical support obligations beyond the scope of the support plan, if any, specifically purchased by the Applicant; or
 - any losses arising from the Applicant’s architecture, deployment, configurations, third-party integrations, or operational management of workloads.

- The Applicant acknowledges that Google Cloud Platform services are provided by Google, and CAIN does not independently warrant or guarantee the uninterrupted availability, performance, or fitness of such services.

•

• **Article 3 Application and Acceptance of the Services**

•

- In accordance with the provisions of Article 1, the Applicant shall apply for the Services to CAIN using the prescribed application.
- If CAIN requests the submission of materials necessary to determine whether to accept or reject the Applicant's application for the Services, the Applicant shall submit such materials to CAIN.
- If CAIN determines that the Applicant falls under any of the following items, CAIN may reject the application for the Services use.
 - If there are any omissions or other deficiencies in the application contents, or if the application contains any omissions or misrepresentations,, or if other false facts are declared at the time of application.
 - If there is a risk of failing to fulfill the obligations stipulated in these Terms of Use.
 - If you have acted in violation of these Terms of Use in the past.
 - In the event that there are facts contrary to the representations or assurances set forth in Article 23.
 - In cases where there is a hindrance to our business, or in other cases where CAIN deems it inappropriate.
- If CAIN accepts an application from an applicant, CAIN shall notify the Applicant to that effect.

•

• **Article 4 The Applicant Obligations**

•

- Applicant shall accept the Google Cloud Terms of Service (<https://cloud.google.com/terms>) (hereinafter referred to as "TOS").
- Applicant acknowledges and agrees that CAIN and Google are independent contractors and that CAIN is not Google's agent or partner or in a joint venture with Google.

•

• **Article 5 Change of Name or Other Registered Information**

•

- If any of the following events occur, the Applicant shall notify CAIN in writing to that effect in advance.
 - Change of corporate name or trade name
 - Change of representative
 - Change of the location or address of the head office or principal place of business.

- Any other changes to the information submitted in the application to CAIN
- CAIN shall not be liable for any disadvantages or losses incurred by the Applicant as a result of the Applicant's failure to provide such notice as described in the preceding paragraph.

• **Article 6 Changes to the Services Content**

- If the Applicant wishes to change the content of the Services provided by CAIN, the Applicant shall submit the prescribed documents to CAIN, as designated by CAIN.
- The procedures set forth in Article 3 shall apply mutatis mutandis to the changes described in the preceding paragraph.

• **Article 7 Changes to These Terms of Use**

- CAIN may amend or update these Terms of Use from time to time by posting the updated version on CAIN's website or otherwise notifying the Applicant electronically. Unless otherwise stated, such amendments shall become effective upon posting. Continued use of the Services after such effective date shall constitute acceptance of the revised Terms of Use.

• **Article 8 Fees**

- GCP Usage Fee means the monthly amount calculated by Google (in US Dollars) based on the Applicant's usage in the current month and multiplied by the average TTS for the month of usage. The GCP Usage Fee is calculated in Indian Rupee (INR) (hereinafter referred to as "Usage Fee").
- For months in which the usage fee is less than INR 1500, CAIN shall charge a flat rate of INR 1500 as management fee.
- CAIN shall calculate the monthly usage fee for the Applicant at the end of each month and issue an invoice for such fee to the Applicant by the 7th business day of the following month. The Applicant shall pay the full invoice amount to CAIN by the last day of the following month in which the invoice is issued.
- Payment of the fees stipulated in the preceding paragraph shall be made by any of the methods specified in the following items approved by CAIN. All transfer fees and other expenses necessary for payment shall be borne by the Applicant.
- Account transfer
- Bank transfer
- Other methods specified by CAIN.

- If the Applicant unlawfully evades the Services charges or other financial obligations owed to CAIN, the Applicant shall pay to CAIN an amount equal to twice the evaded amount, plus the applicable consumption tax, as a penalty.

Article 10 Late Payment Interest

- If any outstanding amount is not paid by the due date, the Applicant shall pay interest at an annual rate of 18% on the unpaid balance, calculated from the due date until the date the payment is substantially settled.

Article 11 Prohibited Acts and Compliance

- The Applicant shall not engage in any of the following prohibited acts when using the Services:
 - Acts that infringe, or may infringe, upon the personal rights or interests of CAIN or any third party, including but not limited to honor, reputation, or privacy.
 - Acts that infringe, or may infringe, upon the copyrights or other intellectual property rights of CAIN or any third party.
 - Impersonating CAIN or any third party in connection with the use of the Services.
 - Criminal acts; acts that incite, encourage, or facilitate criminal activity; or acts that may lead to criminal conduct.
 - Falsifying, deleting, or tampering with information belonging to CAIN or any third party accessible through the Services.
 - Acts that interfere with, or may interfere with, the provision or operation of the Services.
 - Using the Services in a manner that disrupts or is likely to disrupt the use of the Services by other users.
 - Copying, modifying, reverse engineering, decompiling, adapting, disassembling, or otherwise attempting to extract the source code of software or content provided by CAIN in connection with the Services.
 - Using the Services in connection with the operation of nuclear facilities, air traffic control, life-support systems, or other activities where a failure of the Services could result in loss of life, personal injury, or environmental damage.
 - Creating multiple projects disguised as a single project (involving chargeable resource units such as computing, storage, or network) for the purpose of avoiding fees.
 - Engaging in information processing or storage activities subject to the International Traffic in Arms Regulations (ITAR) issued by the U.S. Department of State.
 - Developing or operating communications services (e.g., applications that

allow end users to make or receive calls over the public switched telephone network) using the Services.

- Illegally using or misappropriating user IDs or passwords.
- Using the Services to distribute or transmit computer programs (including viruses) that interfere with or may interfere with the business operations of others, or providing such programs to third parties.
- Disseminating content related to adult entertainment, obscenity, child pornography, or content deemed inappropriate by CAIN, including material unsuitable for minors.
- Acts that infringe the rights of CAIN or third parties, or that violate applicable laws, regulations, or public order and morality.
- Using the Services in a manner that causes, or is reasonably likely to cause, abnormal resource consumption, excessive billing exposure, infrastructure abuse, unauthorized automated activity, cryptocurrency mining without authorization, or other operational or financial risk to CAIN or Google.
- Any other acts that violate these Terms of Service.

Article 12 Prohibition of Resale

The Applicant shall not resell, engage in resale, or sublicense all or any part of the Services to any third party without prior consent of CAIN.

Article 13 Outsourcing to Third Parties

- CAIN may outsource part of the Services operations to a third party. The Applicant hereby agrees to such outsourcing in advance.
- CAIN may disclose confidential information to such subcontractors to the extent necessary for the performance of the Services. However, CAIN shall ensure that subcontractors are bound by confidentiality obligations equivalent to those set forth in Article 16.

Article 14 Contact and Notification

- Inquiries regarding the Services, responses to other communications from the Applicant to CAIN, and other communications or notifications from CAIN to the Applicant shall be conducted in a manner determined by CAIN.
- If CAIN sends a notification to at least one of the addresses, facsimile numbers, e-mail addresses, or other contact details registered by the Applicant, such notification shall be deemed to have been delivered, even if it does not actually reach the Applicant. The time at which the notification is sent shall be regarded as the date of delivery.
- The Applicant agrees that notices, policies, amendments, Terms of Use updates,

and other legally required communications may be provided electronically through CA's website, email communication, or electronic acceptance workflows.

Article 15 Privacy

- CAIN shall protect the privacy and legal rights of the Applicant in accordance with applicable laws and regulations.
- Personal information shall be handled in accordance with CAIN's personal information protection policy or privacy policy, as applicable.
- CAIN may provide Google with the data submitted by the Applicant through the Services, but not only to the extent necessary for the provision of the Services.

Article 16 Confidentiality

- The Applicant and CAIN shall maintain the confidentiality of any information disclosed by the other party pursuant to these Terms of Use and shall not disclose such information to any third party without the prior consent of the other party.
- The confidentiality obligation set forth in the preceding paragraph shall not apply in the

•
following cases:

- Information that has become publicly known without any breach of these Terms of Use or fault attributable to either party;
- Information lawfully obtained from a third party without a confidentiality obligation;
- Information already held by the receiving party at the time of disclosure;
- Information required to be disclosed by law, government agency, or court order;
- Information provided by CAIN to Google to the extent necessary for the provision of the Services.

Article 17 Maintenance, Suspension, Modification, and Termination of the Services

- In order to maintain the Services in proper working condition, CAIN may temporarily suspend operation and perform maintenance inspections at any time.
- In such cases, CAIN shall, in principle, notify the Applicant in advance; however, in emergencies, CAIN may suspend the Services and conduct maintenance or inspection without prior notice.
- CAIN may also suspend the Services due to unavoidable circumstances, such as unforeseen accidents or force majeure events.
- In the event of a natural disaster, incident, or other emergency situation, or where there is a likelihood of such an event, CAIN may provide necessary information

for disaster prevention, relief, the securing of transportation, communications, electricity supply, or the maintenance of public order. CAIN may also take measures to limit the availability of the Services in order to prioritize communications necessary for the public interest.

- CAIN may add, modify, or discontinue the Services, in whole or in part, upon prior notice to the Applicant.
- CAIN shall not be liable for any damages incurred by the Applicant or any third party as a result of delays, suspensions, or changes in the Services due to the reasons stated in this Article or other similar circumstances.
- CAIN may temporarily suspend all or part of the Services, with or without prior notice, where CAIN reasonably determines that such suspension is necessary to:

1) prevent abnormal, excessive, unusual, or suspicious usage patterns; ② prevent unauthorized access, fraudulent activity, cryptocurrency mining, denial-of-service activity, or other misuse of the Services; ③ protect CAIN, Google, or the Applicant from unexpected or excessive billing exposure, operational risk, security incidents, or legal liability; or ④ maintain the stability, integrity, or security of the Services.

CAIN shall not be liable for any damages, losses, business interruption, or claims arising from any suspension undertaken in good faith pursuant to this Article.

Article 18 Contract Period

- The term of the Services shall be one ① Year from the date of execution of the contract. Unless either party notifies the other of its intention not to renew—by the Applicant at least three ③ days before the expiration of the term, or by CAIN at least seven ⑦ days before the expiration—the Services shall automatically renew for successive one-year terms on the same terms and conditions.
- Upon expiration or termination of the contract, the Applicant shall be responsible for deleting its project(s) on GCP. The Applicant shall remain liable for any usage fees incurred after the end of the contract period due to failure to delete the project(s), as stipulated in these Terms of Use. This provision shall also apply in cases of termination pursuant to Articles 18, 19 and 20.

Article 19 Cancellation by the Applicant

- If the Applicant wishes to cancel the use of the Services, the Applicant shall submit to CAIN a cancellation application request in the form prescribed by CAIN.
- If the Services are canceled pursuant to the preceding paragraph, usage fees up to the date of cancellation shall be calculated on a pro-rata basis, based on the number of days in the month in which the cancellation date falls. However, cer-

tain services, such as agency fees, are excluded.

Article 20 Cancellation by CAIN, Suspension of Use, and Loss of Benefits of Deadline

- If the Applicant falls under any of the following items, CAIN may immediately suspend the provision of all or part of the Services without prior notice. In such cases, CAIN shall not be precluded from claiming damages against the Applicant:
 - The Applicant violates any provision of these Terms of Use.
 - The Applicant makes any false declaration or notification, commits fraud, or engages in any other wrongful act against CAIN.
 - The Services charges are to be paid by account transfer and the payment account designated by the Applicant becomes unavailable due to collection procedures or the actions of a financial institution.
 - A supervisory authority imposes a suspension of business, or revokes the Applicant's business license or registration.
 - A petition for seizure, provisional seizure, provisional disposition, compulsory execution, auction for exercise of a security interest, disposition for tax delinquency, or any equivalent procedure is filed against the Applicant.
 - A petition for the commencement of bankruptcy proceedings, civil rehabilitation proceedings, corporate reorganization proceedings, or special liquidation is filed by or against the Applicant.
 - A bill or check drawn or accepted by the Applicant has been dishonored at least once, or the Applicant has reached a state of suspended payment.
 - The Applicant is dissolved due to merger, capital reduction, abolition or change of business, or a resolution for dissolution.
 - Any event occurs that makes it difficult for the Applicant to fulfill these Terms of Use.
 - A material change occurs in the Applicant's assets, credit, or solvency.
 - If any invoice or payment owed by the Applicant remains unpaid for more than thirty (30) days from the applicable due date, CA may suspend all or part of the Services, including the Applicant's cloud subscriptions, billing account access, or associated services, with or without prior notice, until all outstanding amounts are fully paid.

CAIN shall not be liable for any damages, losses, service interruptions, data loss, business interruption, or claims arising from such suspension.

- If the Applicant falls under any of the items listed in the preceding paragraph, the Applicant shall immediately repay to CAIN all amounts owed at that time in one lump sum.

- If CAIN reasonably determines that the Applicant's use of the Services involves abnormal consumption patterns, excessive billing spikes, unusual resource utilization, suspected compromise of credentials, unauthorized access, fraudulent activity, cryptocurrency mining, security threats, overdue payments more than one month or any activity that may expose CAIN or Google to financial, operational, legal, or reputational risk.

Article 21 Data Deletion upon Termination of Contract

Upon termination of the Services for any reason (including cancellation), CAIN may delete all data stored by the Applicant on its server in connection with the Services. CAIN shall not be liable for any damages incurred by the Applicant or any third party as a result of such deletion.

Article 22 Prohibition of Transfer

The Applicant shall not assign or otherwise transfer any rights or obligations under these Terms of Use to any third party.

Article 23 Exclusion of Antisocial Forces

- The Applicant shall not be liable for any loss or damage arising from the use of the Applicant's own personal information, or that of an agent or intermediary of the Applicant, if the Applicant or the agent or intermediary is currently a member of a crime syndicate, a member of a crime syndicate, a person who has not been a member of a crime syndicate for 5 years, an associate member of a crime syndicate, a company related to a crime syndicate, a general meeting house, a socially motivated group or special intelligent violent group, or any other person equivalent thereto (hereinafter collectively referred to as "Organized Crime Groups"). The Applicant represents and warrants that it does not fall under any of the following categories and will not fall under any of the following categories in the future.
 - Having a relationship where Organized Crime Groups are recognized to have control over management.
 - Having a relationship with any members of the Organized Crime Groups that are deemed to be substantially involved in management.
 - Having a relationship that can be seen as unfairly using members of the Organized Crime Groups, for the purpose of gaining fraudulent profits for oneself, one's own company, or a third party, or for the purpose of causing damage to a third party.
 - Having a relationship that is deemed to be involved in providing funds, etc. or providing benefits to members of the Organized Crime Groups.

- An officer or person substantially involved in management has a socially reprehensible relationship with members of the Organized Crime Group
- If it is found that the Applicant or the person acting as an agent or intermediary of the Applicant is a member of the Organized Crime Group or falls under any one of the items of the preceding paragraph, in violation of the representations or warranties in the preceding paragraph, CAIN may cancel all contracts with the Applicant without prior notice.
- CAIN shall not be liable for any damages incurred by the Applicant as a result of cancellation of the Services used in accordance with this Article 23.

Article 24 Limitation of Liability

- If CAIN fails to provide the Services to the Applicant for reasons attributable to CAIN, CAIN shall compensate the Applicant for damages up to an amount equal to the monthly Service charges for the affected billing month, but only if the Services remain unavailable for a continuous period of at least seventy-two (72) hours from the time CAIN becomes aware of such unavailability, or for an aggregate of at least one hundred-twenty (120) hours in a single billing month. However, if the Applicant does not submit a claim for such compensation by the date that is one month after the date on which the Applicant could have made the claim, the Applicant shall forfeit the right to compensation.
- Any period during which the Services cannot be provided due to scheduled maintenance, suspension, or changes shall not be counted toward the unavailability thresholds described in the preceding paragraph.
- CAIN shall not be liable for any damage, including but not limited to loss, corruption, or leakage of data, arising from the use of the Services or any other network services accessed through the Services, or nor for any damages resulting from information obtained by the Applicant through the Service.

Article 25 Disclaimer

- Except as set forth in Article 24, CAIN shall not be liable for any damages incurred by the Applicant arising out of or in connection with the use of the Services (including, without limitation, loss, damages, or leakage of data stored by the Applicant or use of the Services for purposes other than the intended purpose). The Applicant shall not seek compensation from CAIN for such damages. If the Applicant causes damage to any third party through the use of the Services, the Applicant shall resolve any such damage at its own responsibility and expense.
- CAIN shall be responsible for any damage caused to the Applicant in connection with GCP failures, malfunctions, maintenance inspections, or other Google Cloud services, only in accordance with the terms, scope, and content of the SLA

specified by Google. , and others shall not assume any responsibility, including liability for non-conformity to the contract. Furthermore, the provisions of the preceding paragraph shall not apply to damages to which this paragraph applies, and CAIN shall not be liable as provided in the same paragraph.

- The Applicant acknowledges that the provision of GCP depends on Google and may be subject to the following events, and that CAIN shall have no liability for any loss or damage resulting therefrom:
 - Suspension or termination of all or part of GCP or related services by Google or at Google's direction.
 - Google may change all or part of the GCP service (including deletion of functions) or terminate the GCP service itself.

Article 26 Compensation for Damages

If either the Applicant or CAIN causes damages to the other party due to a breach of these Terms of Use (including any misrepresentation or breach of warranties stipulated in Article 23, such party shall be liable to compensate the other for the damages incurred.

Notwithstanding the foregoing, the maximum liability of CAIN for damages payable to the Applicant shall be limited to the amount of the Usage Fees paid by the Applicant to CAIN for the month immediately preceding the month in which the event giving rise to the damage occurred; provided, however, that this limitation shall not apply in cases where the damages are caused by the intentional misconduct or gross negligence of CAIN or the Applicant.

Article 27 Consultation

Any matters not provided for in these Terms of Use, or any doubts or disputes regarding the interpretation of these Terms of Use, shall be resolved in good faith through consultation between the Applicant and CAIN.

Article 28 Applicable Law

These Terms of Use shall be governed by and construed in accordance with the laws of India.

Article 29 Jurisdiction

In the event of any dispute in connection with the use of the Services, Gurgaon, Haryana, India shall have the exclusive jurisdiction as the court of first instance.

TEAM GATHERING





Accelerated Computing Enterprise Pvt. Ltd.

Delhi NCR

www.c-ace.co | in@cloud-ace.com

Cloud Ace Global | Japan, China, Hong Kong,
Taiwan, Thailand, Vietnam, Singapore, Indonesia,
India, and Brazil.