



# Terms Of Use Comtrade Cloud Service

Comtrade System Integration

16/01/2026

## Content

<b>1. COMTRADE CLOUD SERVICE LEVEL RULES.....</b>	<b>4</b>
1.1 ENSURING SERVICE AVAILABILITY.....	4
1.2 TARGET LEVEL OF SYSTEM AVAILABILITY IN COMTRADE CLOUD SERVICES.....	4
1.3 DEFINITION OF AVAILABILITY AND DURATION OF UNPLANNED OUTAGE.....	4
1.4 RESPONSE TIME IN CASE OF UNPLANNED INCIDENT.....	5
1.5 DIFFERENT LEVELS OF CUSTOMER SUPPORT FOR THE USE OF COMTRADE CLOUD SERVICES .....	6
1.6 SYSTEM MONITORING .....	7
1.7 MONITORED COMPONENTS .....	7
1.8 CILENT MONITORING AND TESTING TOOLS .....	7
1.9 AUTOMATED SYSTEM LOAD .....	7
<b>2. COMTRADE CLOUD SYSTEM RESILIENCE RULES .....</b>	<b>8</b>
2.1 HIGH AVAILABILITY STRATEGY OF COMTRADE CLOUD SERVICES.....	8
2.2 REDUNDANT POWER SUPPLY AND COOLING .....	8
2.3 REDUNDANT SERVER INFRASTRUCTURE .....	8
2.4 REDUNDANT NETWORK INFRASTRUCTURE .....	9
2.5 REDUNDANT STORAGE SYSTEMS .....	9
2.6 BACKUP STRATEGY FOR COMTRADE CLOUD SERVICES .....	9
<b>3. COMTRADE CLOUD SECURITY RULES .....</b>	<b>10</b>
3.1 CUSTOMER ENCRYPTION FOR EXTERNAL CONNECTIONS .....	10
3.2 NETWORK SEGMENTATION .....	10
3.3 NETWORK ACCESS CONTROL .....	10
3.4 NETWORK BANDWIDTH AND LATENCY .....	10
3.5 SECURITY MEASURES.....	10
3.6 SYSTEM ACCESS CONTROL AND PASSWORD MANAGEMENT.....	11
3.7 DATA MANAGEMENT.....	11
3.8 DATA PROTECTION .....	11
3.9 DATA DELETION.....	12
3.10 SECURITY INCIDENT RESPONSE .....	12
3.11 DATA PRIVACY.....	12
3.12 COMPLIANCE WITH ISO STANDARDS.....	13
<b>4. COMTRADE CLOUD SUPPORT RULES .....</b>	<b>14</b>
4.1 COMTRADE CLOUD SUPPORT CONDITIONS.....	14
4.1.1 <i>Support Fees</i> .....	14
4.1.2 <i>Support Period</i> .....	14
4.1.3 <i>Technical Contacts</i> .....	14
4.1.4 <i>Comtrade Cloud Support Services</i> .....	14
4.2 COMTRADE CLOUD CUSTOMER SUPPORT SYSTEMS.....	15
4.2.1 <i>Cloud Customer Support Portal</i> .....	15
4.2.2 <i>Telephone and Email Support</i> .....	15

---

<b>5.</b>	<b>COMTRADE CLOUD CHANGE MANAGEMENT POLICY .....</b>	<b>16</b>
5.1	COMTRADE CLOUD CHANGE MANAGEMENT AND MAINTENACE POLICY .....	16
5.2	EMERGENCY MAINTENANCE .....	17
5.3	MAJOR MAINTENANCE CHANGES .....	17
5.4	DATA CENTER RELOCATION .....	17
<b>6.</b>	<b>COMTRADE CLOUD DISASTER RECOVERY SERVICES POLICY .....</b>	<b>18</b>
6.1	SCOPE .....	18
6.2	SYSTEM RESILIENCE.....	18
6.3	DISASTER RECOVERY .....	18
6.4	RECOVERY TIME OBJECTIVE (RTO) .....	19
6.5	RECOVERY POINT OBJECTIVE (RPO) .....	19
6.6	SERVICE RESTORATION.....	19
6.7	DISASTER RECOVERY PLAN OBJECTIVES .....	19
6.8	PLAN TESTING .....	20
<b>7.</b>	<b>COMTRADE CLOUD SUSPENSION AND TERMINATION POLICY .....</b>	<b>21</b>
7.1	TERMINATION OF CLOUD SERVICES .....	21
7.2	SUSPENSION DUE TO BREACH .....	21

# 1. Comtrade Cloud Service Level Rules

## 1.1 Ensuring service availability

Service availability starts from the moment Comtrade activates the client's Cloud environment, i.e. after the signing of the contract between Comtrade and the Client for the provision of the corresponding Cloud service. After establishing Cloud service, Comtrade will maintain the targeted level of service availability in accordance with the conditions specified below in these Rules.

## 1.2 Target level of system availability in Comtrade Cloud services

Comtrade undertakes that the target level of availability of infrastructure services, i.e. the provision of Cloud services is 99.5% for a period of one calendar year, starting from the moment of activation of the Comtrade Cloud service, except in cases where the Agreement, i.e. the offer states otherwise.

## 1.3 Definition of availability and duration of unplanned outage

Service Availability means that the Client is enabled to log in to and access the Comtrade Cloud services in accordance with the provisions set out below.

“Unplanned Outage Duration” is calculated from the moment Comtrade internally detects, or the Client reports, a complete interruption of service availability, until the moment the service is restored to an operational state and made available to the Client.

“Unplanned Outage Duration” means any period of time during which the services are unavailable, but does not include any period during which the services or any component of the services are unavailable due to the following:

- Partial performance degradation, reduced capacity, or limited service functionality shall not be considered an unplanned outage, unless explicitly defined otherwise by the contract or technical offer;
- Service failures or degradations, or malfunctions resulting from scripts, data, applications, equipment, infrastructure, software, penetration testing, service testing, or monitoring tools directed or performed by the Client;
- Planned downtime, scheduled and announced maintenance, maintenance windows, or downtime performed by Comtrade at the Client's request or in accordance with the Client's instructions for maintenance, configuration activation, backups, or other purposes requiring the service to be temporarily taken offline;
- Downtime resulting from actions taken by Comtrade at the Client's request or in accordance with the Client's instructions;
- Inability to access services or downtime caused by the Client's conduct, including negligence or breach of the Client's material contractual obligations, or other circumstances beyond Comtrade's control;

- Events resulting in service interruption or shutdown due to circumstances that Comtrade reasonably considers to pose a significant threat to the normal operation of the services, operational infrastructure, facilities from which the services are provided, access to, or integrity of the Client's data (e.g., hacker or malware attacks). Any temporary suspension or limitation of the service undertaken to prevent or mitigate a security incident shall be deemed a justified protective measure and shall not be included in the Unplanned Outage Duration;
- Downtime beyond the control of Comtrade and/or the Client caused by natural disasters, severe weather conditions, fire, nuclear incidents, electromagnetic pulse events, terrorist acts, riots, war, arson, rebellion, civil unrest, armed conflicts of any kind, work stoppages, closure of business premises, strikes, shortages, government decisions or restrictions (including refusal or cancellation of any export, import, or other permit), theft, bankruptcy, machinery failures, quarantine, communication failures, power outages, internet or telecommunications outages not caused by Comtrade and/or the Client, epidemics, pandemics, or other events beyond Comtrade's reasonable control and other force majeure events;
- Lack of availability or disproportionately long response times by the Client in reacting to incidents caused by the Client itself or attributable to its fault (e.g., in cases of spamming, distribution of illegal material, or similar illegal activities by the Client), or other Client actions not in compliance with applicable laws and regulations, which require the Client's involvement in identifying or resolving the source of the issue or incident;
- Service unavailability caused by issues on the Internet, third-party networks, third-party cloud services, or integrations not under the direct control of Comtrade shall not be considered an unplanned outage;
- Downtime caused by failures or fluctuations in power, connection, network, or telecommunications equipment or links due to the Client's conduct or circumstances beyond Comtrade's control;
- Downtime caused by system administration, commands, or file transfers performed by the Client's users or representatives;
- Downtime resulting from the Client's equipment, third-party equipment, or software components not under the exclusive control of Comtrade.

## 1.4 Response time in case of unplanned incident

Optimal response time for resolving incident requests may vary significantly depending on the severity of the incident and industry standards; however, in general, the timeframe can be categorized as follows:

- **Critical Priority Incidents (P1):** Incidents that severely disrupt or prevent business processes, such as outages of critical systems or security threats. Response time should be within **1 hour**.
- **High Priority Incidents (P2):** Incidents that affect operations but do not completely prevent business processes. Response time should be within **4 hours**.

- **Medium Priority Incidents (P3):** Incidents affecting a limited number of services or functionalities. Response time should be within **4 to 8 hours**.
- **Low Priority Incidents (P4):** Incidents with minimal or no impact on business operations. Response time should be within **24 hours**.

## 1.5 Different Levels of Customer Support for the Use of Comtrade Cloud Services

Clients have varying needs that require comprehensive support for their use of Cloud services and infrastructure. The primary requirement is a reliable and scalable infrastructure that ensures uninterrupted operation and business continuity. Clients also require faster and more efficient solutions for technical issues, as well as optimization of resource usage to improve efficiency, meet performance requirements, and further reduce costs.

Support services within Comtrade Cloud are flexible, responsive, and highly professional, providing Clients with the confidence and resources needed to maximize their investment in Cloud services.

	Basic	Standard	Premium	Managed
Support Description	It provides basic problem-solving services within Comtrade Cloud's responsibility and is focused on basic Cloud infrastructure	It includes request management and change management in the customer's infrastructure, with faster response times and mid-level prioritization	It provides access to expert technical teams, quick answers to critical questions, personalized service and proactive assistance in the optimization and secure management of cloud infrastructures	It includes overall management and full responsibility for the design and architecture of the user system, adaptation to the specific needs of the client and the project.
Response	Up to 8 hours, without guaranteed time for resolvent	Up to 4 hours for high priority ticket	Up to 1 hours for high priority tickets	Up to 1 hours for high priority tickets
Time	9x5 Monday to Friday excluding national holidays	9x5 Monday to Friday excluding national holidays	24x7	24x7
Priority	Low, tickets with minimal impact on the user's business	Low, tickets with minimal impact on the user's business	High, tickets with critical impact on the user's business	High, tickets with critical impact on the user's business

Communication	Ticketing, email	Ticketing, email	Ticketing, email, phone	Ticketing, email, phone
---------------	------------------	------------------	-------------------------	-------------------------

Table 1. Customer Level Support

## 1.6 System Monitoring

Comtrade uses various software tools to monitor the availability of the subscribed Comtrade Cloud services and the operation of the Comtrade Cloud infrastructure. Monitoring is performed 24x7x365 throughout the year in order to ensure timely detection of incidents, performance degradation, and continuity of service delivery.

## 1.7 Monitored components

Comtrade shall monitor the service infrastructure and, as necessary, generate alerts for **CPU, memory, storage, and network components**. Comtrade shall timely notify the Client and, where applicable, send alerts in the event of deviations from predefined thresholds related to the manner and volume of Cloud service usage, as well as in the event of detected anomalies that may affect the stability, performance, or availability of the services.

Monitoring applies exclusively to infrastructure components under the control of Comtrade and does not include applications, operating systems, configurations, or software components managed by the Client, unless otherwise agreed in writing.

## 1.8 Client Monitoring and Testing Tools

Due to the potential adverse impact on service performance and availability, the Client shall not use its own monitoring or testing tools, including automated user interfaces and web service connections related to any of the Comtrade Cloud services, without the prior written consent of Comtrade.

Comtrade reserves the right to remove, limit, or disable access to any tool, script, or mechanism that violates the above limitations or that, in Comtrade’s reasonable assessment, may negatively affect the stability, performance, or security of the services, without any obligation or liability towards the Client.

Any outages, degradations, or damages resulting from the use of such tools shall not be considered an unplanned service outage nor shall they constitute grounds for exercising any rights agreed under the contract or technical offer.

## 1.9 Automated System Load

The Client shall not use, nor allow the use of, data scraping tools or data collection technologies across the Comtrade Cloud services’ user interface without the explicit prior written approval of Comtrade.

---

## 2. Comtrade Cloud System Resilience Rules

The resilience and backup measures described in these Terms apply exclusively to Comtrade Cloud services. The Client is solely responsible for establishing and maintaining its own business continuity plan to ensure continuity of its operations in the event of a disaster, as well as for the backup and recovery of software not developed or provided by Comtrade through the Cloud services defined with the Client, unless otherwise explicitly specified in the relevant offer.

### 2.1 High Availability Strategy of Comtrade Cloud Services

To ensure business continuity in the event of an incident affecting Comtrade Cloud services, Comtrade utilizes services deployed on redundant computing infrastructure. Comtrade data centers are equipped with redundant components and power supplies with backup generators, which help maintain data center resource availability in the event of an incident, as further described below.

### 2.2 Redundant Power Supply and Cooling

The infrastructure design includes **redundant power supply and distribution** for the data center and rack cabinets within the data center. The Comtrade data center located at **Savski nasip 7, Belgrade, Serbia**, is built and operates in accordance with applicable standards. At other locations where Comtrade provides Cloud services, **colocation data centers** are used, which operate in accordance with their respective certified standards.

Cooling components of the Comtrade data center are also redundant. All elements of the cooling system, including precision air conditioning units and condensers, are designed with a minimum **N+1 redundancy**. The equipment operates **24 hours a day, 365 days a year**. Each air conditioning unit is equipped with its own sensors for temperature and relative humidity, filter contamination, and moisture presence beneath the raised floor.

The data center operates continuously throughout the year and therefore requires permanent cooling and air conditioning. The air conditioning units are interconnected via their control units into a dedicated **LAN network**, enabling communication between control units and alternating operation of devices according to programmed time intervals.

In the event of failure of one or more units or a power supply interruption, the remaining units automatically assume additional load. All parameters such as airflow, cooling capacity, and noise levels are optimized for each unit.

### 2.3 Redundant Server Infrastructure

The server infrastructure of Comtrade Cloud services consists of multiple physical servers on which client services are executed. Redundancy of the server infrastructure is achieved at the level of the physical server or hypervisor, or at the level of the protected application (where applicable).

---

## 2.4 Redundant Network Infrastructure

The Cloud infrastructure network topology includes **redundant links from multiple Internet service providers**, as well as duplicated/redundant firewall and router devices that ensure uninterrupted service delivery in the event of a failure of any single component.

The Comtrade network infrastructure within data centers consists of multiple mutually isolated networks used for the delivery of Comtrade Cloud services to Clients. A layered networking approach is implemented to ensure that Client data is protected across all layers of the **OSI network traffic model**.

## 2.5 Redundant Storage Systems

Data within Comtrade Cloud services is stored in configurations with redundant storage capacity, providing protection against failure of individual disks or disk arrays.

## 2.6 Backup Strategy for Comtrade Cloud Services

As part of its disaster recovery practices, Comtrade performs **periodic backups** of data within the Client's Cloud services exclusively for Comtrade's internal use, to minimize data loss in the event of a disaster.

Backups are retained **online or offline for a minimum of three (3) days** from the date of creation, unless otherwise specified in the contract or offer. Comtrade does not typically perform updates, insertion, deletion, or reconstruction of Client data on behalf of the Client. However, as an exception, and subject to prior written approval and an additional fee, Comtrade may assist the Client in reconstructing data that the Client may have lost because of its own actions.

---

## 3. Comtrade Cloud Security Rules

### 3.1 Customer Encryption for External Connections

Encrypted traffic is used for access to Comtrade Cloud services. Comtrade shall not be responsible for encryption implemented at the level of the Client's services.

### 3.2 Network Segmentation

Comtrade data centers contain isolated networks used for the delivery of Comtrade Cloud services to Comtrade Cloud Clients. A layered networking approach is implemented to protect Client data at the physical layer, as well as at the data link, network, transport, and application layers.

### 3.3 Network Access Control

Authentication, authorization, and account management are implemented through standard security mechanisms designed to ensure that only authorized operations personnel and support engineers have access to the systems.

### 3.4 Network Bandwidth and Latency

Comtrade is not responsible for the Client's network connectivity or for any difficulties or issues arising from or related to the Client's network connection (e.g., bandwidth limitations, excessive latency, temporary network interruptions), or issues caused by the Internet.

Comtrade monitors the operation of its network infrastructure and will work to resolve internal issues that may affect service availability.

### 3.5 Security Measures

Comtrade provides secured IT environments for both office locations and Cloud infrastructure. Common security controls at office locations and colocation/data center facilities include, but are not limited to, the following:

- Physical access requires authorization and is under continuous monitoring;
- All individuals within secured areas must visibly wear official identification;
- Visitors are recorded in a visitor log and may not move freely within the premises without escort or supervision by authorized personnel;
- Management of keys, cards, and other access credentials is controlled, and personnel leaving employment with Comtrade are required to immediately return assigned access credentials.

Additional physical security measures are implemented in Comtrade Cloud data centers and include, among others:

- Continuous video surveillance of critical areas, including entrances, perimeters, and rooms housing infrastructure equipment;

- Physical barriers and controlled access points designed to prevent unauthorized access by individuals and vehicles;
- 24x7x365 access control by trained security personnel, including visual identity verification and visitor escort throughout the data center;
- Segmentation of premises into zones with different security levels, with access restricted exclusively to authorized personnel;
- Logging and auditing of access to infrastructure areas in accordance with internal security procedures.

### 3.6 System Access Control and Password Management

Access to Comtrade Cloud systems is restricted exclusively to authorized personnel in accordance with the **principle of least privilege**. Comtrade enforces strict password policies for infrastructure components and Cloud management systems used to operate the Comtrade Cloud environment. These policies include, among others, requirements for minimum password length and complexity, regular password changes, prevention of password reuse, and technical measures for protecting authentication credentials.

Strong passwords and, where technically feasible, **multi-factor authentication (MFA)** are applied across the infrastructure to reduce the risk of unauthorized access via user accounts.

The Client is fully responsible for managing and administering end-user accounts within its Cloud environment, including defining and enforcing password policies, assigning and restricting access privileges, securely storing access credentials, and timely revoking access for users who no longer require it. Comtrade does not manage, monitor, or assume responsibility for the Client's end-user accounts, nor for the consequences of unauthorized access resulting from deficiencies in the Client's user account management, unless explicitly agreed otherwise.

### 3.7 Data Management

During the use of Comtrade Cloud services, Clients retain control over and responsibility for the management of data residing in the Cloud environment. Client data includes data uploaded or created for use within the Comtrade Cloud services.

The Client shall not provide Comtrade with information related to health data, payment card data, or other sensitive personal information that requires specific legal, regulatory, or business security obligations for processing such data. However, where available for specific Cloud services, Comtrade may offer Clients the option to purchase additional services designed for processing regulated data within the service environment. Such additional services are not available for all Cloud services.

### 3.8 Data Protection

Comtrade Cloud offers several standard encryption technologies and data protection options, depending on the specific Cloud service, for data in transit or at rest. For network transmission, Clients may choose to use a VPN to protect their data in transit over public networks. In addition, Comtrade backups of Client environments represent an encrypted method of storing Client data.

---

## 3.9 Data Deletion

Upon termination of service provision (as described in the Comtrade Cloud suspension and termination rules) or at the Client's request, Comtrade shall delete data residing in the Cloud environment in a manner that ensures such data cannot be reasonably accessed or read, unless there is a legal obligation requiring Comtrade to retain the data or preventing Comtrade from deleting all or part of the data.

## 3.10 Security Incident Response

Comtrade evaluates and responds to incidents that raise suspicion of unauthorized access to or handling of Client data. Comtrade shall notify the Client and cooperate with the Client, relevant technical teams, and competent authorities where required, in order to respond to the incident. The objective of the incident response shall be to restore the confidentiality, integrity, and availability of the Client environment and to identify root causes and remediation steps.

## 3.11 Data Privacy

The Comtrade Cloud Services Agreement defines how Comtrade processes personal data residing in the Comtrade Cloud environment and to which Comtrade may have access in connection with the provision of Cloud services.

Where Comtrade obtains access to personal data in connection with the provision of Cloud services, Comtrade shall process personal data on behalf of and for the account of the Client, solely for the purpose of fulfilling its contractual obligations. Comtrade shall process such data in accordance with the purpose and manner specified by the Client, respecting the Client's written instructions and applying the protective measures prescribed by the Client.

The Client undertakes to instruct Comtrade to process personal data only on the basis of a valid legal ground and, where required, after notifying the competent authority of the processing activities. The Client shall ensure that a valid legal basis for processing exists throughout the entire duration of the processing activity under the Agreement. If the legal basis for processing ceases to exist, the Client shall promptly notify Comtrade thereof. The Client shall reimburse Comtrade for any costs incurred by Comtrade in connection with the processing of personal data.

The contractual parties undertake to apply appropriate technical, organizational, and personnel measures to protect the rights and freedoms of data subjects and to ensure that personal data processing is carried out in accordance with applicable data protection laws, taking into account the nature, scope, context, and purposes of processing, as well as the likelihood and severity of risks to the rights and freedoms of natural persons.

The Client shall implement appropriate technical, organizational, and personnel measures to ensure that only personal data necessary for each specific processing purpose is processed, with regard to the amount of data collected, the extent of processing, the retention period, and data accessibility.

Unless otherwise provided by the Agreement or a separate Data Processing Agreement, Comtrade shall apply its standard personal data protection measures. Any Client requests for additional personal data protection measures shall be subject to negotiation, shall be specifically defined at the conclusion of the Agreement, and shall be subject to additional fees.

Upon fulfillment or termination of the Agreement, the Client shall promptly notify Comtrade whether the personal data that was subject to processing is to be deleted or returned to the Client. If the Client fails to notify Comtrade of further handling of personal data within three (3) months after fulfillment or termination of the Agreement, it shall be deemed that Comtrade has been instructed to delete all copies of personal data processed under the Agreement.

### 3.12 Compliance with ISO Standards

Comtrade Cloud services are compliant with the requirements of the following implemented ISO standards:

- **ISO 9001:2015**
- **ISO/IEC 20000-1:2018**
- **ISO/IEC 27001:2022**
- **ISO/IEC 27017:2015**
- **ISO/IEC 27018:2019**
- **ISO/IEC 27701:2019**

All implemented standards are subject to annual audits of Comtrade's business operations, including Comtrade Cloud services, conducted by reputable certification bodies.

The Client remains solely responsible for its own compliance with applicable laws and regulations when using any Comtrade Cloud service. The Client must inform Comtrade of all technical requirements arising from its legal obligations prior to signing the Agreement. Additional certifications and compliance with specific regulatory frameworks within Comtrade Cloud services may be available for an additional fee.

---

## 4. COMTRADE CLOUD SUPPORT RULES

The support described in these Cloud Support Rules applies exclusively to Comtrade Cloud services and is provided by Comtrade as part of such services, in accordance with the applicable purchase order.

### 4.1 Comtrade Cloud Support Conditions

#### 4.1.1 Support Fees

The fees paid by the Client for the Comtrade Cloud services offer under the purchase order include the support described in these Comtrade Cloud Support Rules. Additional fees may be charged for any additional Comtrade support services purchased by the Client.

#### 4.1.2 Support Period

Comtrade Cloud support becomes available on the service commencement date and ends upon the expiration or termination of the Cloud services in accordance with the purchase order (the “**Support Period**”).

Comtrade shall have no obligation to provide the support described in these Support Rules after the expiration of the Support Period.

#### 4.1.3 Technical Contacts

The Client’s technical contacts represent the sole points of contact between the Client and Comtrade for Comtrade Cloud support services. When submitting service requests, the Client’s technical contact shall have a basic understanding of the reported issue and the ability to reproduce the issue to assist Comtrade in diagnosing and triaging the problem.

To avoid interruptions in support services, the Client shall promptly notify Comtrade whenever there is a change in the person authorized as a technical contact.

#### 4.1.4 Comtrade Cloud Support Services

Comtrade Cloud support services include the following:

- Diagnosis of issues or difficulties related to Comtrade Cloud services;
- Reasonable efforts to resolve reported errors that can be verified within the Comtrade Cloud services, so that such services operate in all material respects;
- Support for technical service-related requests in accordance with the Agreement;
- 24x7 access to the Cloud Customer Support Portal designated by Comtrade and support for logging service-related requests;
- Assistance with non-technical customer service matters during Comtrade’s standard business hours (09:00 to 17:00, local time).

---

## 4.2 Comtrade Cloud Customer Support Systems

### 4.2.1 Cloud Customer Support Portal

As part of the Comtrade Cloud offering purchased by the Client pursuant to the purchase order, Comtrade provides Cloud customer support through a Cloud Customer Support Portal designated for the applicable Cloud service. Access to the Cloud Customer Support Portal is limited to the Client's designated technical contacts and other authorized Cloud service users.

### 4.2.2 Telephone and Email Support

The Client's technical contacts may access telephone support provided by operators via the phone numbers listed on the Comtrade Support website:  
<https://comtradeintegration.com/en/contact/>

Email support is also available to the Client via **support@comtradecloud.com**. In addition, Clients may open support tickets through the designated support portal at:  
**support.comtradecloud.com**

---

## 5. Comtrade Cloud Change Management Policy

### 5.1 Comtrade Cloud Change Management and Maintenance Policy

Comtrade Cloud operations perform changes to Cloud hardware infrastructure, operating software, product software, and related application software in order to maintain the operational stability, availability, security, performance, and currency of the Comtrade Cloud. Comtrade adheres to formal change management procedures to ensure that necessary reviews, testing, and approvals are completed prior to the implementation of any changes in the Comtrade Cloud environment.

Changes executed through change management procedures include system and service maintenance activities, upgrades and updates, and Client-specific changes. Comtrade Cloud change management procedures are designed to minimize service disruptions during the implementation of changes.

Comtrade reserves specific maintenance windows for changes that may require Cloud services to be unavailable during the maintenance period. Comtrade endeavors to ensure that change management procedures are carried out within scheduled maintenance windows, taking into account periods of low traffic.

Comtrade will endeavor to provide advance notice of any modifications to the standard maintenance schedule. For Client-specific changes and updates, where feasible, Comtrade will endeavor to coordinate maintenance windows with the Client.

For changes expected to cause service interruptions, Comtrade will endeavor to provide advance notice of the expected impact. The duration of scheduled maintenance windows shall not be included in the calculation of Unplanned Downtime Duration within the monthly Availability Level measurement period. Comtrade shall use commercially reasonable efforts to minimize the use of such reserved maintenance windows and the duration of maintenance activities that cause service interruptions.

Comtrade reserves the right, from time to time, to make changes, replacements, or enhancements to certain tools, software solutions, and other technical components used in the provision of Cloud services, for the purpose of improving functionality, security, regulatory compliance, or infrastructure optimization, as well as in the event of changes in commercial terms, including pricing changes, imposed by vendors or third parties whose services, products, or technologies are necessary for the provision of Cloud services. Such changes and/or modifications may result in changes to the technical characteristics and/or service levels of Cloud services, as well as an increase in the price of Cloud services to the end user, whereby the applicable service price shall be increased by the amount of the difference arising from the application of such changes and/or modifications, of which the end user shall be timely notified.

---

## 5.2 Emergency Maintenance

Comtrade may periodically be required to perform emergency maintenance in order to protect the security, performance, availability, or stability of the Comtrade Cloud environment. Emergency maintenance may include software patches or core system maintenance, as required. Comtrade endeavors to minimize the need for emergency maintenance and will endeavor to provide notice at least 24 hours in advance of any emergency maintenance that requires service interruption.

## 5.3 Major Maintenance Changes

In order to help ensure continuous stability, availability, security, and performance of Cloud services, Comtrade reserves the right to perform major changes to its hardware infrastructure, operating software, application software, and supporting application software under its control no more than twice per calendar year. Each such change shall be considered scheduled maintenance and may cause Cloud service unavailability for up to 24 hours. Each such change is intended to occur during a scheduled maintenance window. Comtrade will endeavor to announce the expected unavailability up to 60 days in advance.

## 5.4 Data Center Relocation

Comtrade may relocate services provided to the Client to other production data centers and shall provide the Client with at least 30 days' prior notice thereof, except in the event of a disaster, in which case the disaster recovery plan shall apply.

---

## 6. Comtrade Cloud Disaster Recovery Services Policy

### 6.1 Scope

These Policies apply solely to the Client's services within the Comtrade Cloud. The activities described in these Terms do not apply to the Client's own disaster recovery, business continuity, or backup plans or activities, and the Client is responsible for archiving and reconstructing all software not produced by Comtrade.

The purpose of Disaster Recovery Services is to provide the ability to restore services in the event of a major disaster, as designated by Comtrade, that results in the loss of a data center and the unavailability of the relevant service.

For the purposes of these Policies, a "disaster" means an unplanned event or issue that causes a complete loss of access to the location used to provide Comtrade Cloud services, rendering the Client's Cloud environment at that location unavailable.

### 6.2 System Resilience

Comtrade Cloud services provide infrastructure that includes a comprehensive data backup strategy. Comtrade Cloud includes redundant capabilities such as power supplies, cooling systems, telecommunications services, networking, application domains, data storage, and physical and virtual servers.

Comtrade shall initiate the disaster recovery plan in accordance with these Terms upon declaration of a disaster and shall endeavor to recover production data and use reasonable efforts to re-establish the production environment. Backups are intended solely for Comtrade's use in the event of a disaster.

### 6.3 Disaster Recovery

Following a disaster, Comtrade shall provide recovery and reconstruction of its production Cloud services to the most recently available state.

Comtrade has established alternative Cloud environment locations that enable full operational capability in the event of service loss at a location. Comtrade maintains a Disaster Recovery Plan that describes reconstruction procedures.

Disaster recovery operations apply to physical loss of infrastructure at Comtrade facilities. Comtrade reserves the right to determine when to activate the Disaster Recovery Plan. During the execution of the Disaster Recovery Plan, Comtrade shall provide Clients with regular status notifications.

## 6.4 Recovery Time Objective (RTO)

The Recovery Time Objective (RTO) represents Comtrade's target for the maximum period between the decision to activate recovery processes in accordance with these Policies to bridge service failure and transition to an alternative location following a declared disaster, and the point at which the Client may resume production operations in the backup production environment. If the decision to bridge service failure is made during an ongoing upgrade process, the RTO shall be extended to include the time required to complete the upgrade. The RTO shall be no less than 12 hours from the declaration of the disaster.

## 6.5 Recovery Point Objective (RPO)

The Recovery Point Objective (RPO) represents Comtrade's target for the maximum period during which data may be lost in the event of a disaster. The RPO shall be no more than 24 hours from the occurrence of the disaster, excluding any data entries that may have been in progress at the time the disaster occurred.

## 6.6 Service Restoration

These Policies identify the purpose and scope of the Disaster Recovery Plan, roles and responsibilities, management commitment, coordination among organizational entities, and compliance requirements. The Plan documents procedures for restoring Cloud services in the event of a disaster.

Comtrade is committed to minimizing the duration of interruptions caused by disasters or equipment failures. As an expression of this commitment, Comtrade maintains a Cloud environment business continuity disaster recovery plan for the timely recovery and restoration of Comtrade operations.

## 6.7 Disaster Recovery Plan Objectives

The objectives of the Comtrade Disaster Recovery Plan for Comtrade Cloud services are:

- In emergency situations, Comtrade's primary priority and objective is the health and safety of people.
- Maximizing the effectiveness of contingency operations through an established Disaster Recovery Plan consisting of the following phases:
  - **Phase 1 – Disaster Recovery Activation Authorization Phase** – detection of service interruption or failure at the location, assessment of damage scope, and plan activation.
  - **Phase 2 – Recovery Phase** – reconstruction of temporary IT operations at an alternative location.
  - **Phase 3 – Reconstruction Phase** – restoration of processing capacity and continuation of operations at the location.

- 
- Identification of activities, resources, and procedures required to meet processing requirements during extended outages.
  - Assignment of responsibilities to appropriate personnel and provision of recovery guidelines during extended outages.
  - Ensuring coordination with other personnel responsible for disaster recovery planning strategies, as well as coordination with external points of contact, external service providers, and execution of this plan.

## 6.8 Plan Testing

The Cloud services disaster recovery plan is tested annually, either as a practical exercise or a tabletop exercise. Tests are used for staff training and are coordinated with all personnel responsible for contingency planning and operations.

The tests verify that online backups can be recovered and that procedures for transferring services to an alternative processing location are adequate and effective. Test results are used to improve processes and initiate corrective actions.

---

## 7. Comtrade Cloud Suspension and Termination Policy

### 7.1 Termination of Cloud Services

Upon termination or expiration of services pursuant to a purchase order or at the Client's request, Comtrade shall delete or otherwise render inaccessible the production environments and data contained therein in a manner designed to prevent access or reading, unless there is a legal obligation preventing Comtrade from deleting the entire environments or parts thereof.

For a period of up to 15 days following termination or expiration of services pursuant to a purchase order, Comtrade shall make production data available to the Client for retrieval. Comtrade shall have no obligation to retain Client data after the expiration of this 15-day post-termination period. Comtrade Client support identifiers shall be revoked upon expiration of the 15-day period, and Comtrade shall remove or render inaccessible the Client's data within the service.

Pilot environments of Comtrade Cloud services are subject to the same termination rules as standard production environments.

Upon service termination, if the Client requires Comtrade's assistance to access the Comtrade secure server for the purpose of retrieving production data, the Client must submit a request through the Cloud Client Support Portal related to this service.

As part of the service termination process, Comtrade shall provide secure protocols through which users designated by the Client may transfer the Client's data from the Cloud service.

### 7.2 Suspension Due to Breach

If Comtrade detects a breach or is contacted regarding a breach of the terms and conditions of the Comtrade Cloud Services Agreement or acceptable use policies, Comtrade shall take measures including, without limitation, suspension of access to the user account, suspension of access to the administrative account, or suspension of the environment until the issues are resolved.

Comtrade shall use reasonable efforts to restore the Client's services as soon as possible after Comtrade determines, at its sole discretion, that the issues have been resolved or the situation has been remedied.



[comtradeintegration.com](http://comtradeintegration.com)