ConMas i-Reporter
Cloud Service Level

Ver1.5　2020.8

CIMTOPS Corporation.
ConMas i-Reporter Cloud Operations Group

Document Objectives

This document has been crafted with the assumption that it will be utilized by the customer for the purpose of considering the implementation of the i-Reporter cloud version service. Within the customer's internal procedures, it describes the security response status of the i-Reporter cloud version service, which conforms to the Ministry of Economy, Trade, and Industry cloud service checklist and will be necessary when reporting to the system management or security examination department.

Should any issues or concerns not be resolved through the information provided henceforth, please do not hesitate to inquire further through appropriate sales representative channels. Additionally, please understand that it may take within a week or so to respond to each individual inquiry, and that during peak periods, more time may be required to respond than usual.

Revision history

July 1, 2019
ver0.1 release

October 23, 2019
ver1.1 release
Updates to annual and multi-month usage, and added information regarding mid-term cancellation

November 12, 2019
ver1.2 release
Update to past operational rate performance, added information regarding RPO, and changed minimum response time to inquiries to within 3 business days.

February 10, 2020
ver1.3 release
Address change, and minor revisions

May 27, 2020
ver1.4 release
Updated the number of companies and users that have adopted the system to April of the current year.

Security policy, efforts, and responses regarding i-Reporter.

■ Security Policies

CIMTOPS Corporation. positions the information security basic policy (https://www.cimtops.co.jp/security/) published as the highest policy and conducts information security management activities in all areas of product planning, development, sales, operation monitoring, and support in accordance with the scope of ISMS (ISO/IEC 27001:2014).

■ Efforts and Responses

In terms of ISMS management, we implement design and programming that takes into account the security environment, including secure development. At the same time, we implement the following in order to respond to changes in the environment surrounding security:

- **Daily collection and evaluation of information related to security**
- **Dissemination and sharing of security information that is evaluated as emergency or critical and the consideration of countermeasures**
- **Prompt implementation of trial application when necessary for security measures**
- **Undergoing vulnerability diagnosis by third-party organizations at least once a year and prompt implementation of necessary corrective actions**
- **24-hour, 365-day manned monitoring**

ISMS activities undergo internal and external audits at least once a year to maintain and improve the level of security. In addition, we have established the necessary internal system to provide support through a sophisticated support web, notifying customers through electronic mail in the event of an incident that leads to service interruption.

By working together as a team, we are consistently focused on maintaining and improving the utmost level of information security.

Company information and track record of service

Company Name	CIMTOPS Corporation
Establishment Date	1991-10-01
Board of Directors	CEO: Takashi Mizuno
	Director in charge of Manufacturing Solutions: Osamu Mukouyama
	Director in charge of i-Reporter & MC-Web Controller: Daisuke Namazue
	Part-time Director: Haruhisa Gai
	Part-time Director: Kunio Sakurai
Business Description	Development and sales of production scheduler and production management system, DIRECTOR, for custom production orders
	Development and sales of paperless "on-site" recording, reporting, and viewing solution, ConMas i-Reporter
	Development and sales of MC-Web CONTROLLER, which easily IoT-ifies any existing manufacturer's machinery and equipment and collects, monitors, aggregates, and analyzes detailed operation status
	Development and sales of BOP process editor, MPPCreator, for considering and creating M-BOM and manufacturing processes in coordination with E-BOM
	Development and sales of other production management related software
	System integration related to the above and system consulting
Headquarters Location	Shinagawa-ku, Tokyo 2-25-2 Kamiosaki, Shinagawa Tokyu Building 10F, 141-0021 Japan
Phone	03-5721-4610
Fax	03-3491-4610
Offices/Affiliates	Central Area Office, Kariya Seminar Room, West Japan Area Office, Shanghai Office
Cloud Service Name	i-Reporter Cloud Version Service
Service Type	SaaS (Software as a Service)
Service Contents	The i-Reporter Cloud Service, provided by CIMTOPS Corporation, is a SaaS service hosted on the Azure platform within the Japanese region, allowing users to utilize the i-Reporter system via the internet. The service includes the ConMas Designer for inputting report designs, user registration and access management, management of designed reports, and access log management with the ConMas Manager, as well as storage area for various data and server functions necessary for using i-Reporter, all on the cloud. As of December 2023, the service has been implemented in 3,151 companies, including listed companies, with 145,012 users.

Outline of i-Reporter Cloud Edition Service Terms of Use

Please refer to the following text for details regarding the terms of service:
This service provides server space for the storage of customers' electronic data, as well as certain software functions constructed on the server, and tools for managing stored electronic data.

Service Features Offered	In the case of monthly usage, the service is specified as a basic service for one month starting from the following month of contract signing, and then automatically renewed.
	In the case of annual usage, the service is specified as a one-year service starting from the following month of contract signing, and a new order will also be required for the following year.
	In the case of multi-month usage, the service is specified as a period determined starting from the following month of contract signing, and if continuation is desired, an order for the next period will be required before the 25th of the expiring month.
Terms of Service	In the case of monthly usage, the service will be terminated upon notification of termination before the 25th of the desired month.
	In the case of annual or multi-month usage, the service will expire upon termination of the contract before the 25th of the contract end month.
Service Cancellation Procedure	In the case of monthly usage, you must notify us of your desire to terminate your service one month before your desired cancellation, otherwise the service will automatically renew.
	In the case of annual or multi-month usage, you must notify us of your desire to cancel before the 25th of the desired month. Please understand that refunds for already paid fees will not be granted under any circumstances.
Cancellation During the Subscription Period	At the start of usage, support will be provided upon confirmation of the ID and password issued by our company by the "person in charge" registered at that time. Support inquiries via the support web will be accepted 24 hours/365 days. Responses to inquiries will be provided according to our company's separate regulations for days, weekdays, and time zones.
Support	As stipulated in the i-Reporter Cloud Service Terms of Use, we do not detect whether the information handled contains "personal information," "specified p
Handling of Personal Information and Confidential Information	Customers are responsible for managing backups of data used by i-Reporter and records related to i-Reporter access and processing.
Executive Responsibility of Data Management	Cloud Service performs maintenance to improve service operation. During maintenance, the system may be temporarily suspended or some functions may not be available.
	We will notify the registrar via e-mail approximately one week prior to the maintenance.
Discontinuation of Service	In the unlikely event that we discontinue our cloud services, we will notify you at least 3 months prior to the scheduled discontinuation date via the means provided by us.

Outline of i-Reporter Cloud Edition Service Terms of Use

Suspension of Service	We guarantee that we will not suspend the service for more than 24 consecutive hours.
	In the event of service interruption for more than 24 consecutive hours due to a malfunction of the service network installed by MHI, compensation will be provided at the option of MHI, but will be determined by MHI in accordance with the conditions stipulated in the General Terms and Conditions.
	Compensation may not be provided in some cases.
Scope of Compensation	The terms and conditions of the service and usage, as well as the conditions for termination of contract, can be found in the Cloud Service Terms of Use.
Exclusions of liability and terms of contract termination	The laws of Japan shall be applicable and the jurisdiction for any disputes shall be under the scope of the Tokyo District Court.

Certification

■ **Physical Access Control in the Data Center**

- As a service infrastructure for providing the i-Reporter Cloud version service, we use multiple domestic data centers of the Microsoft Azure service (here in after referred to as Azure) in Japan.
- Azure is widely used worldwide and maintains extremely high reliability and security, which can be viewed in detail on the following Microsoft website: (https://docs.microsoft.com/ja-jp/azure/security/azure-physical-security).

Azure's Third-Party Certifications Azure holds certifications such as FISC, CS MARK(Gold), ISO20000, ISO27001, ISO27017, and ISO27018 among others.
For more information, please refer to the information published on the following Microsoft website: (https://www.microsoft.com/ja-jp/trustcenter/compliance/complianceofferings)

■ **Third-Party Certifications Held by CIMTOPS Corporation.**

- Our company holds ISO/IEC27001 certification and applies security policies, organization, and systems, as well as management strategies.

ISO/IEC27001
JUSE-IR-412
(認証範囲:本社)

ISMS-AC
ISMS ISR005

The Ministry of Economy, Trade and Industry guidelines for Cloud Service Level Checklist.

METI Cloud Service Level Checklist Correspondence Table 1/7

No.	Classification	Service Level Item Examples	Official-regulations	Support Availability	Content
Application Operations					
1	Possible occurrences	Service downtime	The service operating hours, including scheduled maintenance for equipment and network inspections/upkeep.	○	The service is generally available during regular business hours, but maintenance may be scheduled for up to 7 hours per month, typically between 11pm and 6am. (This does not include planned or regularly scheduled maintenance.)
2		Notification of planned outages	Prior notification of scheduled maintenance outages (including description of timing/method of prior notification)	○	Regular maintenance interruptions will be communicated to registered contacts via email notification at least five business days in advance, as well as through the maintenance information page on our support website (https://cimtops-support.com/i-Reporter/ja/24-news-jp/2-conmas-i-Reporter-web).
3		Advance notice of service termination	Confirmation of prior notification when service provision is terminated (including description of timing/method of prior notification)	○	As stated in the Terms and Conditions of Service we will notify you at least 3 months prior to service termination.
4		Measures to be taken in the event of sudden service termination	Measures in place for safeguarding program and system configurations and data in the event of sudden service interruption	○	In the event of sudden service interruption, while we always prioritize the protection of our clients' data, we will make every effort to restore the system within our capabilities. As for client data,we kindly request that it is backed up at the responsibility of the client.
5		Service rate of operation	Service usage rate (scheduled service time - downtime) / scheduled service time)		Not disclosed to the public. FY 2018 Actual availability rate of 99.5% (not including scheduled maintenance)
6		Disaster recovery	System recovery/support system in the event of a disaster		Disaster recovery is not supported.
7		Alternate measures in the event of major disruption	Alternative measures when early recovery is not possible		No alternative method is provided. i-Reporter terminals (iPads and other devices can be used for offline data entry).
8		Data formats provided as alternative measures	Defines the data format provided in as alternative measures	○	Customer data can be downloaded from ConMas Manager in CSV format or from ConMas Designer in XML format at the customer's own risk. You can also download the created form data (in PDF/Excel or CSV format if the form data is in Excel) from ConMas Manager. Data management is the sole responsibility of the customer.
9		Upgrade policy	Version updates/change management /patch management policies	○	The program is updated about once a month, and at least 15 days' notice is given on the Support Web site. All relevant parties will be notified of the decision to implement the program via email roughly 5 business days prior to the date of the update.

METI Cloud Service Level Checklist Correspondence Table 2/7

No.	Classification	Service Level Item Examples	Official-regulations	Support Availability	Content
Application Operations					
10	Authentication	Mean time to repair (MTTR)	The average time to repair from the occurrence of a failure (sum of repair times ÷ number of failures)		Not set
11		Recovery Time Objective (RTO)	The target time for resuming service after the occurrence of a failure		Not set
		Recovery Time Objective (RPO)	The target time for backup generation management corresponding to the resumption of service after the occurrence of a failure	○	The data will be restored using the backup data before 1:00 a.m. the previous day or 1:00 a.m. two days prior. However, if the backup has not been completed by that time, the data from up until 11:59 p.m. on the Saturday of the previous week may be used.
12		Number of incidents	The number of failures that occurred in one year / the number of failures that required a long time (over 1 day) to respond to in one year		Not disclosed
13		System audit standards	Monitoring based on the set monitoring standards (monitoring content / monitoring and notification standards)		The system does not currently have a monitoring and audit standard in place.
14		Incident notification process	Communication process at the time of failure (notification destination / method / route)	○	Upon the occurrence of an incident, our company promptly notifies the designated personnel and takes action. Our customers are informed via email notification to the registered contact person.
15		Incident notification time	The time until designated contacts are notified after detection of an abnormal condition or occurrence		We do not have a set protocol, but we make every effort to notify as quickly as possible
16		Incident monitoring interval	The interval for collecting / aggregating failure incidents	○	Ongoing monitoring
17		Report/interval of service availability	The method / interval for reporting service availability	○	Individual reports are not provided. In the event that notification is necessary, notifications and reports will be sent to the registered contact via email.
18		Log acquisition	Types of logs available to users (access logs, operation logs, error logs, etc.)	○	The usage status of i-Reporter system for customers can be obtained from ConMas Manager. Server system logs are generally not provided.
19	Performance	Response time	Response time of processing		Not disclosed
20		Delay	Duration of continued delay in response time of processing		Not disclosed
21		Batch processing time	Response time of batch processing		Not disclosed

METI Cloud Service Level Checklist Correspondence Table 3/7

No.	Classification	Service Level Item Examples	Official-regulations	Support Availability	Content
Application Operations					
22	Augmentability	Customizability	Conditions and information required for customization (modifications), including items/scope/specifications that can be customized (changed)		In principle, customization is not supported.
23		External Connectivity	Connection specifications (APIs, development languages, etc.) with existing systems and external systems such as other cloud computing services	○	An API is available as an option to access i-Reporter system functions from external services.
24		Number of concurrent users	Number of online users who can connect and use the service at the same time	○	There is no limit to the number of concurrent users.
25		Maximum resources provided	Disk space limits/page view limits	○	The amount of storage space to be used is determined at the time of contract. There is a limit to the available storage capacity. (Can be increased as a paid option.)
Support					
26	Service availability (Fault handling)		Time needed to carry out inquiries when responding to a failure	○	We accept inquiries 24 hours a day, 365 days a year. (email and inquiry form)
27	Service Hours (General Inquiries)		Time needed to carry out inquiries when responding to a failure	○	The normal support hours are from 9:30 to 18:00 on weekdays (excluding national holidays, year-end and New Year holidays, etc.). We will endeavor to reply within 3 business days after confirming the contents of the inquiry.

METI Cloud Service Level Checklist Correspondence Table 4/7

No.	Service Level Item Examples	Official-regulations	Support Availability	Content
Application Operations				
28	Backup Methods	Handling of data that belongs to the user, including backup details (frequency, restoration method, etc.), data storage location/format, user access rights to data, etc.	○	The data used in the i-Reporter system is to be downloaded and stored by the customer under their own responsibility via ConMas Manager/ConMas Designer. The system's overall data backup is performed on a daily, weekly, and monthly basis at a remote data center within the country, however, access to this data by the customer is not possible.
29	Timing to retrieve backup data RPO)	When retrieving and securing backup data		The backup of the entire system data is done daily, weekly and monthly intervals at a distant data center within the country, however, customers do not have access to this data. In the event of recovery timing, backups are done for the previous day and the day before that up until 1am of the current day. If the backup is not completed by then, the backup will be from the previous week.
30	Retention period of backup data	Storage period of media with backed up data	○	It will be kept for the duration of the customer's contract.
31	Requirements for data erasure	Whether/when data will be erased, whether/when storage media will be destroyed, and how data that belongs to the user, such as data migration, will be erased after service termination.	○	It is the customer's responsibility to delete the data used in the i-Reporter system from ConMas Manager/ConMas Designer. Data for the entire infrastructure system will be deleted if necessary. However, the data cannot be physically destroyed.
32	Number of backup generations	Number of backup generations secured	○	The i-Reporter system utilizes data that is the responsibility of the customer to download and back up via ConMas Manager/ConMas Designer. While our infrastructure does not guarantee data backup, we do implement daily backups at 1:00 AM, with a retention of 2 generations for the current day and the previous day. Additionally, weekly and monthly backups are taken on Sundays and the first Sunday of the month, respectively. These images are stored separately as weekly and monthly backups.
33	Encryption requirements for data protection	The availability of encryption requirements for the protection of data.	○	Internet connections are encrypted by SSL.

METI Cloud Service Level Checklist Correspondence Table 5/7

No.	Service Level Item Examples	Official-regulations	Support Availability	Content
Application Operations				
34	Key management requirements for multi-tenant storage	The availability and contents of key management requirements for multi-tenant storage encryption.	○	Individual key management is in place.
35	Compensation/insurance in case of data leakage/destruction	The presence or absence of compensation/insurance for data leakage/destruction.		We do not have liability insurance. Customer data management is the sole responsibility of the customer under the terms and conditions of service.
36	Data portability in case of termination	The presence of a system in place that ensures the prompt and complete return of original data upon termination, or the responsibility and means to securely erase data to eliminate concerns of external leakage.	○	It is the customer's responsibility to download the data used for the cloud service before cancellation and then delete it. We will carry out the data deletion operation.
37	Integrity verification operations for deposited data	The method for verifying that the integrity of data is implemented and the task of confirming the verification report is conducted.	○	It is the customer's responsibility to verify the data contents.
38	Restrictive functions for input data format	Availability of input data format restrictions	○	You can use the input data restriction function provided by i-Reporter.

METI Cloud Service Level Checklist Correspondence Table 6/7

No.	Service Level Item Examples	Official-regulations	Support Availability	Content
Application Operations				
39	Requirements for Public Certification	Handling of data that belongs to the user, including backup details (frequency, restoration method, etc.), data storage location/format, user access rights to data, etc.	○	Apart from customer data, server storage is backed up on a daily, weekly, or monthly basis and stored at a remote data center in Japan. However, this data cannot be accessed by the customer.
40	Third-party evaluation of applications	Performed third-party web application vulnerability assessment		At least once a year, the company undergoes a vulnerability inspection by a third party, receives a report on the inspection, and conducts an evaluation and response.
41	Third-party evaluation of applications	Deadline for storing media with data backed up.	○	Backup data is stored for the duration of the customer contract.
42	Encryption level of communication	Encryption strength of communications exchanged with the system	○	Backup data will be kept for the duration of the contract with the customer.
43	Confirmation of information security-related issues in audit reports	The following materials are to be provided to the auditor during the audit of information security-related matters in the auditor's report: "the most recent SAS 70 Type 2 audit report" and "the most recent Audit Report No. 18.		Not supported.
44	Security measures under multi-tenancy	Isolation of information between different user companies, localization of effects of failures, etc.	○	Each customer's contracted space is operated in a completely separate data area.
45	Restriction of information handlers	The number of users who can access the user's data must be limited, and the same restrictions on access as those stipulated by the user's organization must be achieved.	○	In accordance with ISO 27001 certification standards, access privileges are limited to a limited number of persons, and the scope of access is determined for each person. Access within the company, including physical access, is recorded and audited.

METI Cloud Service Level Checklist Correspondence Table 7/7

No.	Service Level Item Examples	Official-regulations	Support Availability	Content
Application Operations				
46	Traceability in case of security incidents	IDs can be used for log searches, and logs are stored for an appropriate period of time. Is the storage period of the logs of an appropriate duration secured, and is the log Is the log provided within an acceptable period of time according to the user's needs?	○	iAccess logs to the i-Reporter system can be viewed by the customer through ConMas Manager. The entire system can be logged at regular intervals to verify records, but customers do not have direct access to the system.
47	Virus scanning	Frequency of virus scanning	○	Virus checks are performed on a regular basis.
48	Security measures for secondary storage media	Backup media, etc., must be kept in encrypted form at all times, data must be completely erased and verified at the time of disposal, and measures such as disabling USB ports and restricting data extraction must be implemented.	○	No secondary storage media is used and backups are made between data centers.
49	Policies for external storage of data	Do you understand the restrictions on data handling and use under the various legal systems of the data storage location?	○	We understand