CELLOPOINT
Secure Your Email

CODLP Cellopoint Online Data Loss Prevention Service Level Agreement (SLA)

Cloud Service Customer (CSC): CODLP End User (Party A)
Cloud Service Provider (CSP): Cellopoint International Corporation (Party B)

1.1 Purpose and Scope

This Agreement is intended to govern the terms and conditions of the "Cellopoint Online Data Loss Prevention Service", including information security controls, personal data protection, data processing, and the responsibilities of both parties. The Service shall be provided in accordance with the best practices specified in ISO/IEC 27017:2015 and ISO/IEC 27018:2019.

By applying for this service, you acknowledge that you have read, understood, and agreed to all the terms and conditions of this Service Level Agreement provided by Party B.

1.2 Definitions

1.2.1 Roles of Both Parties

- Personally Identifiable Information (PII): As defined in ISO/IEC 29100.
- Controller / Processor: Party A acts as the PII Controller, and Party B acts as the Processor.

1.2.2 The Cloud Service provides Data Loss Prevention (DLP) for outbound emails, including email auditing and email encryption.

1.2.3 Cloud service-related information is stored in Japan, Singapore, or Taiwan. The data centers are classified as Tier 5A facilities.

1.3 Service Availability

1.3.1 "Service Availability" refers to the ability to establish SMTP (port 25) connections through the "Cellopoint Online Data Loss Prevention Service", as measured by the "Cellopoint Monitoring System".

1.3.2 The "Cellopoint Online Data Loss Prevention Service " provides 99.9% Service Availability, calculated on a 30-day monthly cycle.

1.3.3 "Service Interruption" refers to a period during which the " Cellopoint Online Data Loss Prevention Service" is unable to forward Party A's emails for more than

ten (10) consecutive minutes (600 seconds).

1.3.4 If a Service Interruption causes Service Availability to fall below 99.9%, Party A may request compensation in accordance with Clause 1.5.1, Service Credits.

1.3.5 Periods of Service Interruption caused by Scheduled Maintenance shall be excluded from Service Availability calculations.

1.4 Email Delivery and Latency

1.4.1 The detailed SMTP records and emails in quarantine for 95% of emails can be viewed in the " Cellopoint Online Data Loss Prevention Service " within five (5) minutes of receipt.

1.4.2 Processing latency refers to the time from receipt of a request to the attempt to transmit the request. HTTP GET requests/responses larger than 1 MB, DLP analysis, and streaming traffic are excluded.

1.5 Service Credits

1.5.1 The service credit standards for the " Cellopoint Online Data Loss Prevention Service" are as follows:

Monthly Service Availability	Service Credits
<99.9% to ≥99.0%	3 day
<99.0% to ≥95.0%	7 day
<95.0%	15 day

1.5.2 The maximum service credit shall not exceed fifteen (15) days per month.

1.5.3 Party A must submit a written request for compensation within seven (7) business days of the Service Interruption. Failure to do so shall be deemed a waiver of the right to claim compensation.

1.6 Technical Support

1.6.1 The " Cellopoint Online Data Loss Prevention Service " provides telephone support from 9:00 AM to 6:00 PM (GMT+8). Outside these hours, Party A may seek support via email only.

1.6.2 Technical Support Response Times

Priority Level	Description	Response Time
Critical	Service outage	Within 2 hours
High	Partial service interruption	Within 4 hours
Low	General issues and suggestions that do not affect service	Within 8 hours

1.7 Application for Subscription or Service Termination

1.7.1 To apply for this service, Party A may submit an application through the official website (https://www.cellopoint.com/) or a dedicated service provided by Cellopoint International Corporation, and complete the registration process in accordance with the user registration and identity verification mechanisms required by Party B.

1.7.2 When subscribing to this service, the service items and quantities selected by Party A through Party B's cloud platform (including the management console, API management interface, or partner channels) shall serve as the basis for the subscription. The subscription effective date shall be the time when Party A successfully submits the application through the platform and Party B's system confirms its completion.

1.7.3 During the subscription period, Party A shall apply for accounts by completing the cloud account application form provided by Party B, or by providing the required information for assistance from Party B's personnel.

1.7.4 If Party A wishes to terminate this service, Party A shall log in to Party B's cloud service platform or notify Party B of the termination request. The termination effective date shall be determined by the time when Party B's system completes the "Termination Confirmation" process. The actual subscription period and applicable fees shall also be calculated based on the records maintained in Party B's system.

1.7.5 Upon service termination, Party B shall provide a data transfer method, remove all data and backups, and provide a record certifying the completion of data deletion.

1.7.6 Party B shall provide mechanisms for data export and deletion, and complete the process within thirty (30) days after service termination.

1.8 Information Security and Privacy Responsibilities

1.8.1 Security Responsibilities:

	CSP	CSC
	Cloud Service Provider	Cloud Service Customer
Email security scanning platform provisioning and maintenance	R/A	I
Threat intelligence and scanning rule updates	R/A	I
Real-time email scanning, blocking, and quarantine	R	I

Cloud Service Provider (CSP) security incident notification and reporting	R	A
Cloud Service Customer (CSC) security incident notification and reporting	A	R
Customer-side security policy configuration	C	R/A
User account and access control management	I	R/A
User education and security awareness training	C	R/A
Compliance policy configuration and enforcement	C	R/A
Security incident monitoring and response	C	R/A
Periodic security policy review and adjustment	I	R/A
Technical support and consultation	R	C
Definitions of Responsibility Codes		
R = Responsible (The party who executes the task)		
A = Accountable (The party ultimately answerable for the task)		
C = Consulted (The party providing input or consultation)		
I = Informed (The party kept updated on progress or outcomes)		

1.8.2 All data shall be encrypted both at rest and in transit. Access controls and multi-factor authentication (MFA) shall be implemented where feasible.

1.8.3 Personal Data Processing:

(1) Data shall only be processed in accordance with the customer's authorization and shall not be used for any other purposes.

(2) In the event of a security incident, the customer shall be proactively notified within 72 hours.

1.8.4 Incident Retention and Log Management: Party B shall establish audit logging mechanisms for critical systems (including cloud services and personal data processed through cloud services) to record user activities (including those of administrators and operators), abnormal conditions, and other information security-related events. Such logs shall be retained for 180 days to facilitate future incident investigations and access control audits.

1.8.5 Third-Party Vendor Management: If Party B uses third-party technology services, Party B shall ensure that such services meet the information security

requirements equivalent to those stipulated in this Agreement and shall manage such vendors in accordance with its vendor management standard operating procedures.

1.9 Audit Mechanism

1.9.1 If Party A needs to conduct an audit or inspection (on-site or remotely), Party A shall notify Party B at least three months in advance to allow Party B sufficient time to provide the necessary assistance.

1.9.2 If Party B has obtained third-party certifications, Party B may provide the relevant certification certificates as an alternative to an on-site inspection.

1.10 Confidentiality and Liability

1.10.1 Both parties shall be responsible for maintaining the confidentiality of sensitive information under this Agreement. In the event of any violation of information security requirements or disclosure of personally identifiable information (PII), the breaching party shall bear the corresponding legal liabilities and compensation obligations.