PRESERVICA GLOBAL ACCEPTABLE USE POLICY

1 Scope and Purpose.

1.1 This policy applies to all cloud-based versions of Preservica including Starter, Starter Plus, Professional, Professional Plus, Enterprise, Enterprise Plus (EPC), Enterprise Plus (EPCP) across all territories.

1.2 This policy applies to the Client and its Authorised Users who must always comply with its provisions to protect the Services from unauthorized access, misuse, and harm.

1.3 This Policy is intended to supplement the provisions of the Client's existing policies on the usage of the Client's information and communications systems by imposing additional obligations on Authorised Users.

1.4 This policy is not intended to eliminate or undermine any existing obligations to which the Client's employees are subject to.

2 Definitions.

2.1 Definitions of defined terms can be found in the applicable Terms and Conditions.

3 Prohibited Use.

3.1 Authorised Users may not:

3.1.1 attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software or the Documentation in any form or media or by any means; nor

3.1.2 attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software; nor

3.1.3 use the Services or the Documentation to provide or sell services to third-parties; nor

3.1.4 license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services or the Documentation available to any third-party; nor

3.1.5 share access of all or any part of the Services with any party or persons; nor

3.1.6 access without authority, interfere with, manipulate, damage or disrupt all or any part of the Services or any equipment or network owned or used by any third-party, or assist any third-party in doing such acts; nor

3.1.7 access, store, distribute or transmit any Viruses during its use of the Services; nor

3.1.8 infringe any Intellectual Property Rights through its use of the Services; nor

3.1.9 access any data that that does not belong to the Client; nor

3.1.10 perform any actions including probe, scan, monitor, performance benchmark or test the Services that in any way that may disrupt, degrade or disable the Services without the prior written consent from Preservica.

4 Fair Use and Usage Limits.

4.1 Use of the Services by Authorised Users is subject to the following fair use and usage limits unless otherwise agree with Preservica:

4.1.1 Ingest rate limits, whichever limit is met first:

Limit per Service	Starter	Starter Plus	Professional	Professional Plus	Enterprise	Enterprise Plus (EPC)	Enterprise Plus (EPCP)
Ingest (Records Per Day)	10,000	10,000	50,000	100,000	100,000	150,000	200,000
Ingest (Data Volume Per Day)	5Gb	250Gb	250Gb	500Gb	500Gb	750Gb	1Tb
Ingest (Data Volume Per Month)	5Gb	1Tb	5Tb	10Tb	10Tb	15Tb	20Tb

4.1.2 API limits, whichever is met first:

Limit per Service	Starter	Starter Plus	Professional	Professional Plus	Enterprise	Enterprise Plus (EPC)	Enterprise Plus (EPCP)
OAI-PMH API	API Not Available	API Not Available	API Not Available	Fair-use	Unlimited	Unlimited	Unlimited
CMIS API	API Not Available	API Not Available	API Not Available	Fair-use	Unlimited	Unlimited	Unlimited
Other API Usage (Read Operations)	API Not Available	API Not Available	API Not Available	200 per 15 minutes	Unlimited	Unlimited	Unlimited
Other API Usage (Write Operations)	API Not Available	API Not Available	API Not Available	100 per 15 minutes	Unlimited	Unlimited	Unlimited
Total API Operations	API Not Available	API Not Available	API Not Available	200 per 15 minutes	Unlimited	Unlimited	Unlimited

4.2 "Fair Use" shall be defined by the reasonable and prudent person standard.

4.3 Preservica reserves the right to suspend access to the Services in line with the Suspension of Services clause in the applicable Terms and Conditions.

5 Security.

5.1 The Client Administrator shall ensure that:

5.1.1 each Authorised User is a named individual; and

5.1.2 the Client Administrator must allocate each Authorized User with individual login details and assign their rights and permissions to enable them to access the services; and

5.1.3 Authorized Users must keep their login credentials confidential; and

5.1.4 Authorized Users may only upload Client Data which they are responsible for and have the legal right to do so; and

5.1.5 they are aware of and execute their responsibilities for Security as outlined in the Shared Responsibility Model.

5.2 The Client shall require that Authorized Users report any breach (or suspected breach) of the Services or this Policy immediately to the Client Administrator, who in turn shall report it to Preservica.

6 Prohibited Client Data.

6.1 Client Data that is ingested, uploaded, transmitted or sent via the Services must not:

6.1.1 be defamatory, abusive, deceptive or threatening or invasive or any person's privacy; nor

6.1.2 breach any legal requirements or contain pornographic or illegal data; nor

6.1.3 promote discrimination based on race, sex, religion, nationality, sexual orientation or age; nor

6.1.4 infringe any person's intellectual property rights; nor

6.1.5 breach any duty owed to any third party, including a duty of confidence; nor

6.1.6 give the impression that it emanates or is endorsed by Preservica if this is not the case.

6.2 The ultimate responsibility for Client Data is that of the Client.