

ABB GENERAL TERMS AND CONDITIONS
FOR PURCHASE OF IT SERVICES
CLOUD SCHEDULE (2026-05)

1. ADDITIONAL DEFINITIONS

In addition to the definitions set out in Clause 1 of the GTC, the following definitions shall apply in this Service Specific Schedule:

“Access Term”: means the term for which Customer is to be provided the Cloud Services, as specified in the Order;

“Cloud Services”: means those Services provided by Supplier which are indicated in the Order as being provided on a "Software as a Service", "SaaS", "PaaS", "IaaS" or "Cloud" basis or where the Order references this Schedule;

“Customer Cloud Content”: means data (which may be Customer Materials and include Personal Data) which are stored on the Cloud Services and/or used, and/or processed by Supplier;

“Disaster”: means any occurrence that may be, or may lead to, an unplanned business interruption or disruption or otherwise impairs the ability of Supplier to perform any of the Services;

“Disaster Recovery Plan”: means a plan that sets out the procedures to be adopted by Supplier in the event of a Disaster (including procedures for planning and preparing for such event);

“Documentation”: means the documentation provided to Customer by Supplier in connection with the Cloud Services and/or the Cloud Software, including the Specification and any user manuals or other materials in any format provided under the Contract, and including any documentation described in the Order;

“Implementation Services”: means the activities described in the Order and any other activities reasonably necessary (other than those expressly assigned to Customer in the Order) to implement, configure and/or connect the Cloud Services;

“Maintenance Release”: means a release of the Cloud Software which corrects faults, adds functionality or otherwise amends or upgrades the Cloud Software;

“Modification”: means any Maintenance Release or Customer specific modification.

2. APPLICATION

This Service Specific Schedule applies to any Services to be provided by Supplier which are Cloud Services, as set out in the Order.

3. IMPLEMENTATION

3.1 Supplier must perform all of the Implementation Services.

3.2 Except as otherwise agreed in the Order, Implementation Services are subject to Customer's acceptance. Supplier shall provide the Implementation Services in a timely manner and ensure that any milestone or deadline dates specified in the Order are met.

3.3 Supplier shall provide Customer with regular progress reports that (in reasonable detail) describe the status of the Implementation Services and identify any actual or anticipated

problems or delays (together with details of all actions being taken or to be taken to remedy such problems or delays).

4. CLOUD SERVICES

4.1 Unless otherwise agreed in writing, which agreement may require additional data privacy agreements to be concluded, Supplier shall provide the Cloud Services in accordance with the Contract. Supplier must provide the Cloud Services from facilities, and using IT architecture and personnel, that are based in the EU, EEA or Switzerland.

4.2 Supplier grants to Customer and each member of the Customer Group, during the Access Term, a worldwide, royalty-free, non-exclusive license to:

4.2.1 use the Cloud Services;

4.2.2 access and use the Cloud Software via the Cloud Services; and

4.2.3 use the Cloud Software (and the Documentation) in relation to any business activity of the Customer Group.

4.3 Customer may permit any Third Party Provider to exercise Customer's rights solely for the purpose of such Third Party Provider providing goods, software and/or services to the Customer Group.

4.4 Customer acknowledges that it has no right, title or interest in the Cloud Software or the Documentation except as set out in the Contract.

4.5 Except as permitted under the Contract, Customer must not:

4.5.1 distribute, sub-license or otherwise transfer all or any part of the Cloud Software to any other person;

4.5.2 exceed usage limits (e.g. the maximum number of authorised users) as and if specified in the Order;

4.5.3 use the Cloud Software as a service bureau or in any similar activity for the benefit of any person who is not a member of the Customer Group;

4.5.4 reverse engineer, decompile or disassemble the Cloud Software except as permitted by applicable laws;

4.5.5 remove, obliterate or alter any copyright, proprietary or similar notices on the Cloud Software; or

4.5.6 intentionally access, store, distribute or transmit any viruses or other malicious software, or any material during the course of its use of the Cloud Services that:

a) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

b) facilitates illegal activity;

c) depicts sexually explicit images;

d) promotes unlawful violence;

e) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or

f) in a manner that is otherwise illegal or causes damage or injury to any person or property.

5. CUSTOMER CLOUD CONTENT

5.1 Notwithstanding Clause 10.1 of the GTC:

5.1.1 Customer Cloud Content will be and remain the property of Customer;

5.1.2 Supplier and Supplier's Team must not use, access, store, copy, or disclose any Customer Cloud Content except as necessary for the performance of its obligations under the Contract or as otherwise expressly authorised in writing by Customer.

5.2 Upon Customer's written request and, in any event, upon expiry or termination of the Contract, Supplier shall free of charge (i) return to Customer and/or make available for export the Customer Cloud Content in a commonly used, machine-readable format, and (ii) delete or permanently erase the Customer Cloud Content from Supplier's systems and provide written certification of deletion. Customer Cloud Content stored in backups that cannot be deleted using reasonable efforts may be retained solely in accordance with Supplier's documented backup retention policy and shall remain subject to the confidentiality and security obligations under the Contract until deleted in the ordinary course.

5.3 Customer shall indemnify and hold Supplier harmless from and against all costs, claims, demands, liabilities, expenses, damages or losses arising out of any third-party claim alleging that Supplier's use of the Customer Cloud Content in accordance with the Contract infringes such third party's Intellectual Property Rights, provided that (i) Supplier gives Customer prompt written notice of the claim, (ii) Customer is given sole control of the defence and settlement of the claim (subject to Supplier's right to participate with its own counsel at its own cost), and (iii) Supplier provides reasonable co-operation at Customer's cost. Customer shall have no liability under this Clause 5.4 to the extent the claim arises from Supplier's use of the Customer Cloud Content other than in accordance with the Contract.

6. CLOUD WARRANTIES

6.1 In addition to any warranties given by Supplier in the GTC, Supplier represents, warrants and undertakes that the Cloud Services as a whole and any individual Modification during the term of the Contract will:

6.1.1 be free from material defects; and

6.1.2 comply and perform in accordance with the Documentation.

6.2 Without limiting Clause 6.1, Supplier represents, warrants and undertakes that each Modification will not degrade the functionality or performance of the Cloud Software.

6.3 Supplier represents, warrants and undertakes that, when delivered to Customer or otherwise implemented by Supplier under the Contract:

6.3.1 it will not insert or include, or permit or cause any person or software to insert or include, any Malicious Software into the Cloud Software as a whole or any individual Modification;

6.3.2 it will use up-to-date, industry accepted anti-virus software to check for and prevent any malicious software or viruses being introduced into the Cloud Software as a whole or any individual Modification; and

6.3.3 it will co-operate with Customer to mitigate the effect of any malicious software or viruses found in the Cloud Software as a whole or any individual Modification.

6.4 Any AI Solution that is embedded in Cloud Software or Cloud Services observes and complies with the same access rights configuration that apply to such Cloud Software or Cloud Services.

6.5 Supplier represents and warrants that it has obtained, and undertakes that it will maintain during the Access Term, all consents, licences and permissions required by it to perform its obligations under the Contract.

6.6 Supplier represents, warrants and undertakes that except as otherwise agreed in the Order, the Cloud Services will comply with security standards, controls and requirements as set out in ISO 27001:2013, SOC 1 type II and/or SOC 2 type II including its availability trust principles.

6.7 The remedies set out in Clause 6.2 of the GTC shall apply.

7. CLOUD SECURITY AND AUDIT OBLIGATIONS

7.1 Supplier shall:

7.1.1 on an annual basis or alternate frequency agreed otherwise, ensure and document that logical accesses are reviewed for need and that unused accounts are removed and provide Customer with a written summary evidencing completion of such reviews

7.1.2 perform a formal application penetration test by a reputable third-party provider annually for all applications provided to Customer or supporting the supply process. Supplier shall provide Customer, upon request, an executive summary of the test results and a remediation plan for any high or critical findings and shall remediate such findings within commercially reasonable timeframes appropriate to the severity.

7.2 Supplier at its sole cost will cause a licensed provider of attestation and compliance services to provide Customer and its auditors once a year an ISO 27001:2013 certification and/ or ISO 27001:2022 certification, SOC 2 Type II and additionally SOC 1 Type II (if supporting Customer financial statement processing) audit report on controls placed in operation and tests of operating effectiveness at Supplier's and Supplier's service providers' facilities with respect to the Cloud Services.

7.3 Any such certifications and audit reports as per Clause 7.2, and any such other information as required by Customer that Supplier prepares as a standard matter for its other customers, will be provided at no additional cost to Customer.

7.4 Supplier must have business continuity and Disaster Recovery Plans and processes in place to ensure the service for Customer is adequately maintained in the event of any negative impact on the Supplier's service.

7.5 Supplier shall comply with the additional security, audit and reporting requirements, if any, specified in the Order.

8. DATA PROTECTION

8.1 Customer acknowledges that it has all right, title and interest in and to the Customer Cloud Content (including personal data) and shall have sole responsibility for (i) the legality, integrity and appropriateness of the data; (ii) the completeness, accuracy, reliability and quality of the data; (iii) obtaining and maintaining the necessary licenses and consents required to use the data (if any) in accordance with the applicable data protection laws; (iv) entering of the data into Cloud Services.

8.2. Customer grants Supplier the right to process Customer Cloud Content as required for the performance the Services, including where necessary, to transfer Customer Cloud Content to third parties for the provision of Services, subject to the terms of these GTC.

9. EXIT SUPPORT

Upon the termination or expiration of the Agreement, the Supplier shall provide the following exit support services:

9.1. Facilitate the export of all Customer Materials and relevant configurations in a commonly accepted, machine-readable format to ensure an effective transition.

9.2. Revoke all access credentials, user accounts, and API keys associated with the Customer to safeguard data security.

9.3. Supply system audit logs, access logs, and relevant compliance documentation for up to ninety (90) days or as agreed between both parties, following termination, upon request, to assist in regulatory compliance.

9.4. Provide reasonable transition support for up to ninety (90) days or as agreed between both parties, which will include technical assistance, documentation handover, and knowledge transfer to either a new service provider or the Customer's internal team.

9.5. Disclose any significant third-party licensing agreements, platform dependencies, or subcontractor relationships that may impact the transition process.

