

## Schedule A: AccessCloud Terms and Implementation

### 1. AccessCloud Terms.

- 1.1. **Access to Platform.** The Subscriber shall complete the registration process for the AccessCloud Platform in the manner specified on the Portal (or via other instructions from SwiftConnect). SwiftConnect shall grant the Subscriber access to and use of the AccessCloud Platform upon completion of the Professional Services and the Subscriber's completion of such account registration process.
- 1.2. **Subscriber-Side Control Systems.** The Subscriber acknowledges that the AccessCloud Platform relies on integrations, via the Platform APIs, to Access Control Systems and other systems and data that, as between the Parties, are under the control of the Subscriber. The Subscriber agrees to provide SwiftConnect access to, and to maintain, such systems as follows:
- a) **Specified Platform-Integrated Systems.** Based on information provided by the Subscriber, the Platform-Integrated Systems that control Restricted Areas at issue, and that are necessary for the Subscriber's intended use of the AccessCloud Platform, are listed on the Product Order (each a "**Subscriber-Side Control System**").
  - b) **Supporting Systems.** The Subscriber acknowledges and agrees (i) that the Subscriber-Side Control Systems include a range of additional inputs and integrations for the Subscriber's applicable Access Control Systems, including but not limiting to inputs from and integrations with (a) database directories of personnel, (b) solutions for provisioning mobile credential and employee credential solutions and applications; (c) identity management systems; (d) tenant and employee engagement apps; (e) print servers; (f) card readers; and (g) mobile device management applications (collectively, "**Supporting Systems**"); (ii) that the term "Subscriber-Side Control Systems" includes such Supporting Systems; and (iii) that its obligations under this Section 1.2 (Subscriber-Side Control Systems) apply to Supporting Systems. The Supporting Systems are listed on the Product Order, or can reasonably be identified via the Product Order by an individual with knowledge of Access Control Systems.
  - c) **Access to Subscriber-Side Control Systems.** The Subscriber shall provide SwiftConnect with access to the Subscriber-Side Control Systems, including (i) physical and logical access to equipment, servers, and other Subscriber-Side Control System elements that are located in the Office Buildings at issue; and (ii) technical and data-sharing access to the Subscriber-Side Control Systems via applicable APIs or other means specified in the documentation for such Subscriber-Side Control Systems. The Subscriber shall be responsible for enabling network connectivity for the AccessCloud Platform to interface with required Subscriber-Side Control System elements that are located in the Office Buildings at issue. For Office Buildings where the Subscriber is not the owner of the property, or the property manager (or other designee) acting on the owner's behalf with respect to the property, the Subscriber shall be responsible for obtaining necessary consents from the landlord (or other interested parties) with respect to SwiftConnect's access to Restricted Areas controlled by the landlord (or such other interested parties), and to the Subscriber-Side Control Systems applicable to such Restricted Areas.
  - d) **Supported Versions.** During the Term, the Subscriber is solely responsible for ensuring that it is using a version of each Subscriber-Side Control System that is supported by, and remains under maintenance from, the provider of such Subscriber-Side Control System (a "**Supported Version**"). SwiftConnect is not responsible for any performance errors resulting from or related to the Subscriber's failure to maintain a Supported Version of each Subscriber-Side Control System. Subscriber shall notify SwiftConnect at least 30 days in advance of any modification, including upgrades, to a system or component connected to the AccessCloud Platform that could reasonably be expected to impact the AccessCloud Platform's performance.
  - e) **Responsibilities concerning Subscriber-Side Control Systems.** The Subscriber is responsible, at its sole cost, for the operation, maintenance, and availability of the Subscriber-Side Control Systems. SwiftConnect is not responsible for any performance errors resulting from or related to the Subscriber's failure to operate, maintain, or make available the Subscriber-Side Control Systems. The Subscriber shall similarly be responsible for license fees (including per seat user fees), subscription fees, certification fees, and other costs and fees associated with such Subscriber-Side Control Systems.
  - f) **Subscriber Access to Portal.** The Subscriber shall ensure that the Subscriber Internal Systems comply with SwiftConnect's system requirements or, if system requirements are not provided, ensure that such Subscriber Internal Systems comply with system requirements that an engineer with reasonable skill would infer from the AccessCloud Platform architecture.
- 1.3. **Uninterrupted Ingress and Egress.** SwiftConnect has architected the AccessCloud Platform such that, if the AccessCloud Platform is unavailable, this unavailability will not hinder or affect the operation of the Subscriber-Side Control Systems or the functioning of the Credential and Mobile Wallet. Accordingly, if the AccessCloud Platform is unavailable, Credentialed Users will continue to be able to exercise their Access Privileges at Restricted Areas in the same manner as if the AccessCloud Platform were available. The Subscriber acknowledges, however, that for the period when the AccessCloud Platform is unavailable, the Subscriber will not be able to access the Portal or the functionality of the AccessCloud API for the uses and purposes set out in Section 3 (Portal) and Section 4 (AccessCloud API) of Appendix 1 to this Schedule A (Configured Platform and Platform-Integrated Systems). Remedies for and other terms governing the availability of the AccessCloud Platform are set out in Schedule C: Service Level Agreement.
- 1.4. **Branding; Private Labeling.** If the Subscriber wishes to include its Marks and branding on components of the AccessCloud Platform, Transaction reports, or other materials associated with its use of the AccessCloud Platform and SwiftConnect agrees to such inclusion and branding, then (i) the Subscriber's Marks for such purpose will be listed in Appendix 2 (Subscriber Trademarks) or otherwise made available to SwiftConnect, and (ii) the Master Terms will govern the protections the Subscriber's Marks will receive. If the Subscriber wishes to private-label the AccessCloud Platform for its Eligible Users and Credentialed Users and SwiftConnect agrees to such

inclusion and branding, then Appendix 2 (Subscriber Trademarks) will so specify, and SwiftConnect will refrain from including its Marks or other branding as to the Subscriber's instance of the AccessCloud Platform; provided, however that in all instances, SwiftConnect shall be entitled to affix one or more of SwiftConnect's Marks to each component of the AccessCloud Platform, the mobile card artwork as accessed by the Subscriber's Eligible Users and Credentialed Users, Transaction Log Reports made available to the Subscriber, and to other materials made available to the Subscriber or its Eligible Users and Credentialed Users.

- 1.5. Privacy Practices.** Subscriber acknowledges that: (i) SwiftConnect's use of Onboarding Information and Transaction Logs in accordance with this Agreement complies with the Subscriber's privacy policy; and (ii) the Subscriber obtains sufficient consent from, and provides sufficient notice to, Eligible Users and Credentialed Users as to its privacy practices (as set out in such privacy policy), all in accordance with Applicable Law.
- 1.6. Use of Credentials.** SwiftConnect represents and warrants to the Subscriber that: (i) it will associate the Credential with no device other than the Mobile Wallet to which such Credential is registered; and (ii) the Credentials will permit only the Access Privileges that the Subscriber has specified in the manner set out in the Portal or in the Access Control System. The Subscriber acknowledges that, through no fault of SwiftConnect, persons or entities other than the Credentialed User might obtain access to the Credentialed User's Mobile Wallet and/or Credential (by permission or by phishing or other fraudulent means). Accordingly, in addition to other disclaimers in this Agreement, SwiftConnect does not provide assurance, and expressly disclaims any such assurance, that the person or entity using a Mobile Wallet and/or Credential is in fact the Credentialed User.
- 2. Participation in Certifications.** The Subscriber acknowledges that, in connection with integrating Subscriber-Side Control Systems with the AccessCloud Platform, SwiftConnect may be obligated to obtain certifications, perform testing, or engage in other activities required by the providers of such Subscriber-Side Control Systems. The Subscriber agrees to participate in such testing, certification, or implementation, as deemed necessary by SwiftConnect (collectively, "**Certification Activities**"). If the Certification Activities primarily concern the Subscriber's specific Subscriber-Side Control Systems, the Subscriber shall be responsible for its costs associated with such Certification Activities. If the Certification Activities are generally applicable to Access Control Systems, and useful generally to SwiftConnect's subscriber base, then SwiftConnect will reimburse the Subscriber for its reasonable out-of-pocket costs associated with such Certification Activities.
- 3. Professional Services.**

  - 3.1. Professional Services.** The Office Building, or the leased space within the Office Building, where SwiftConnect is to implement the AccessCloud Platform is identified in the applicable Product Order. SwiftConnect shall integrate the AccessCloud Platform with the Subscriber-Side Control Systems for such Office Buildings in accordance with the Implementation Plan. The Subscriber shall timely perform its obligations set out in the Implementation Plan and shall otherwise provide SwiftConnect with reasonable assistance in connection with SwiftConnect's execution of the Implementation Plan.
  - 3.2. Access to Subscriber-Side Control Systems.** The Subscriber shall provide SwiftConnect with physical and logical access to Subscriber-Side Control Systems that serve the Office Buildings. Such access shall include access to physical locations where needed, and the Subscriber shall be responsible for obtaining permissions from applicable landlords or others needed for such access, as further specified herein. The Subscriber shall obtain such access in a timely manner, good and sufficient to permit SwiftConnect to meet the milestones set out in the Implementation Plan.
  - 3.3. Milestone Schedule; Subscriber Delays.** SwiftConnect shall use commercially reasonable efforts to complete the Professional Services in accordance with the milestone schedule included in the Implementation Plan (the "**Milestone Schedule**"). Subscriber acknowledges that delays in its assistance and inputs to the Professional Services may, in turn, delay SwiftConnect's completion of tasks under the Milestone Schedule, and Subscriber agrees that its delay will afford SwiftConnect an extension on the target completion dates set out in the Milestone Schedule.
  - 3.4. Project Management.** The Parties' respective Project Leads will be responsible for coordinating each Party's contributions to the Professional Services, and the Parties will use commercially reasonable efforts to preserve continuity in their Project Leads.
  - 3.5. Acceptance of Professional Services.**

    - a) Acceptance Testing.** SwiftConnect shall notify the Subscriber when the SwiftConnect Platform is ready for its review and testing under the Implementation Plan (a "**Review Notice**"). Upon receipt of a Review Notice, the Subscriber shall timely (in keeping with reasonable industry practice) examine and test the SwiftConnect Platform, and SwiftConnect shall provide Subscriber with reasonable training and assistance in order for Subscriber to conduct a meaningful review and set of acceptance tests. If the SwiftConnect Platform complies with good industry practice and otherwise meets the reasonable satisfaction of Subscriber ("**Acceptance Criteria**"), Subscriber shall notify SwiftConnect in writing of its acceptance. If the SwiftConnect Platform fails to meet the Acceptance Criteria, then Subscriber shall notify SwiftConnect of the non-compliance and provide supporting detail. If the Subscriber does not notify SwiftConnect in writing of its acceptance or does not notify SwiftConnect that the SwiftConnect Platform fails to meet the Acceptance Criteria within a reasonable period of time (not to exceed ten (10) business days), or if the Subscriber provisions, registers, or otherwise permits more than fifty (50) Eligible Users or Credentialed Users to access or use the SwiftConnect Platform, the SwiftConnect Platform shall be deemed accepted for all purposes under this Agreement.
    - b) Cure by SwiftConnect.** Upon receipt of a notice of non-compliance under Section 3.5.a) (Acceptance Testing), SwiftConnect shall cure the non-compliant issues identified in such notice in a timely manner, at SwiftConnect's sole cost and expense, and resubmit the corrected deliverables to the Subscriber. The Parties shall then repeat the acceptance process under this Section

3.5 (Acceptance of Professional Services); provided, however, that the Subscriber shall not be obligated to re-test the deliverables more than twice.

- 3.6. No Effect on Warranty and Other Performance Obligations.** The Subscriber's acceptance of the Professional Services under this Section 3.5 (Acceptance of Professional Services) shall not negate or excuse SwiftConnect's required compliance with its representations, warranties, and performance obligations under this Agreement.

---

### Appendix 1 to Schedule A: Configured Platform Features

- 1. Credentialing Users.** The AccessCloud Platform will create and assign Credentials to users as follows:
  - a) Eligible Users; Onboarding Information.** The Subscriber shall identify its Eligible Users via the Portal or other method that SwiftConnect makes available to the Subscriber for such purpose, and shall provide the information concerning such Eligible Users specified by SwiftConnect. Eligible Users must also present Onboarding Information to SwiftConnect in connection with the credentialing process.
  - b) Specifying Access Privileges.** In connection with providing Onboarding Information, the Subscriber shall indicate, via the Portal or other method that SwiftConnect makes available to the Subscriber, the Access Privileges to which the Eligible User is entitled. Such Access Privileges shall apply to both Restricted Areas controlled by an Access Control System managed by a landlord or by a tenant.
  - c) Provision of SwiftConnect Mobile App; Issuance of Credential; Placement in Mobile Wallet.** Upon receipt of requisite Onboarding Information, and the Eligible User's completion of other specified onboarding steps, SwiftConnect will make mobile functionality available to the Eligible user via the SwiftConnect Mobile App specified in Appendix 1 (Configured Platform and Platform-Integrated Systems). When the Eligible User downloads and completes associated instructions concerning the SwiftConnect Mobile App, SwiftConnect will (i) create a unique Credential for the Eligible User; (ii) register that Credential to the Eligible User and designate the Eligible User as a "Credentialed User" for purposes of this Agreement; (iii) assign to the Credential the Access Privileges the Subscriber has specified; and (iv) place the Credential in the Mobile Wallet of the Credentialed User.
- 2. Transaction Logs.** SwiftConnect will maintain logs of interactions between a Credential and relevant Subscriber-Side Control Systems (each a "Transaction"). These logs will include (i) whether the Credential was accepted or declined by the Subscriber-Side Control System; (ii) the Transactions identified by Mobile Wallet (e.g., iPhone or Apple Watch), by Access Privilege (e.g., full-time employee, contractor, part-time employee, intern, etc.), by Transaction type (e.g., door access or other event), by Transaction status (e.g., successful/declined), by date and time, by location of Restricted Area and by OS type (e.g., iOS or Android); and (iii) other data elements that are specified in the System Documentation or otherwise useful for operation of the AccessCloud Platform (such logs and associated data are collectively referred to as "Transaction Logs").
- 3. Portal.** During the Term, the Subscriber shall be entitled to access and use the Portal. Such uses shall include the following:
  - a) Management of Credentialed Users and Access Privileges.** Through the Portal, the Subscriber shall be entitled to select Eligible Users, modify Access Privileges for Credentialed Users, delete Credentialed Users, and take other associated actions specified in the System Documentation (collectively, "**User Management Instructions**"). SwiftConnect will comply with User Management Instructions properly submitted via the Portal.
  - b) Transaction Log Reports.** The Subscriber shall be entitled to access and download reports of Transactions, with the data elements specified in Section 2 (Transaction Logs) (each a "**Transaction Log Report**").
  - c) Use of Reports.** SwiftConnect grants the Subscriber an irrevocable, transferable, paid-up, worldwide right and license to copy, modify, distribute, display, and otherwise use Transaction Log Reports for all purposes consistent with this Agreement, Applicable Law, and the Subscriber's privacy policy.
- 4. AccessCloud API.** SwiftConnect has developed an API that provides subscribers with automated, real-time (or near real-time) access to Transactions and agreed-upon elements of Transaction Logs (the "**AccessCloud API**"). If specified in Appendix 1 (Configured Platform and Platform-Integrated Systems), SwiftConnect will make the AccessCloud API available to the Subscriber and, with the AccessCloud API (and suitable interconnections with applicable Subscriber-Side Control Systems), the Subscriber will have the technical capability to interact with the AccessCloud Platform independent of the Portal. SwiftConnect may provide consulting services with respect to the Subscriber's use of the AccessCloud API, on separate, mutually agreeable terms.

---

### Appendix 2 to Schedule A: Subscriber Trademarks

[To be included, if applicable]