Staffbase Product-Specific Terms

Customer's use of the Services stated below is subject to these Product-Specific Terms and the Master Subscription Agreement between Customer and Staffbase referencing these Product-Specific Terms (the **"Agreement"**). Terms not expressly defined herein have the meaning given in the Agreement.

1. Front Door Intranet and Employee App

Usage Limits. Employee App is licensed based on the number of Customer employee, contractors and agents ("**Customer Personnel")** that are invited to access the Employee App ("**Invited Users**"). Staffbase will determine the Invited User count based on the data available in the Services. Deactivated Customer Personnel (previously Invited Users) who are no longer engaged or employed by Customer are not counted towards the total of Invited Users. For Customers using SSO integrations, including SCIM, SAML, or OIDC, without a regular sync with the Services of the full invited user base, the ability of Customer's Personnel to log in and register for the Employee App through the integration deems them an Invited User.

Employee App Specific License. The following license terms apply in addition to the license permissions and restrictions in the Agreement. For Employee App, Staffbase grants Customer the non-exclusive, non-transferable, and non-sublicensable right to **(i)** permit Invited Users to a during the Subscription Term to install and use the Employee App; and **(ii)** during the Subscription Term, distribute the Employee App to Invited Users through Apple's App Store, the Google Play Store, or another eligible app store (**"App Store"**) unless downloading or using the Employee App is prohibited by the App Store's terms. Upon any expiry or termination of the Subscription Term, Customer shall, and shall ensure that the Invited Users shall, cease to use and distribute the Employee App.

Customer's App Store Account. When Customer distributes the Employee App via an App Store, Customer may be required to sign up for a specific App Store account. Customer is responsible for complying with any relevant terms of service and requirements of any App Stores related to their App Store account and Customer will maintain the functionality of their App Store account. Where Staffbase supports Customer in distributing or managing the Employee App on Customer's behalf, Customer will ensure Staffbase has appropriate access to Customer's App Store account.

App Store Distribution Support. Staffbase shall use reasonable efforts to support Customer in its App Store submissions, such as providing any needed documentation or information about the Employee App that is available to Staffbase. Unless otherwise agreed in writing, Customer is responsible for the distribution and use of their Employee App in the relevant App Store(s). When Staffbase, on Customer's instructions and behalf, distributes the Employee App via Staffbase's own App Store account, Customer remains responsible for the distribution and use of the Employee App as set out in the Agreement and Customer shall provide Staffbase with all required information necessary for Staffbase to distribute and maintain the Employee App in the App Store (including Customer's Employee App privacy policy and any other information about personal data processing required by the relevant App Store).

New Employee App Versions. From time-to-time, Staffbase may provide new versions of the Employee App to Customer. Customer may lose access to the Employee App if the Employee App is not updated to a newer app version in line with the Documentation. Customer agrees that: **(i)** if Customer distributes the Employee App via App Stores, Customer shall promptly submit updates to the App Store (and within 48 hours for emergency security-related updates), and Customer shall use reasonable efforts to encourage its Invited Users to update the Employee App; **(ii)** if Customer distributes via a channel Customer controls (such as mobile device management, a company internal app store, or a self-hosted download page), Customer shall promptly update the Employee App on the devices it manages (and within 48 hours for emergency security-related updates); **(iii)** if Customer distributes via a download page, Customer will, where relevant, promptly update the Employee App on the relevant download page (and within 48 hours for emergency security-related updates), and Customer must use commercially reasonable efforts to encourage its Authorized Users to update the Employee App; and **(iv)** if Staffbase manages the Employee App on Customer's behalf, Customer shall promptly provide Staffbase with the necessary documentation or provide Staffbase access to Customer's account to update the Employee App. If reasonably required for the security of the Services, Staffbase may disable older versions of the Employee App.

Branding of the Employee App. For certain plans, Staffbase gives Customer the ability to customize the Employee App with Customer's branding. Customer owns all goodwill generated resulting from Staffbase's use of Customer's branding. Any changes to the branding of the Employee App after the initial selection has been made may be subject to additional fees, to be agreed between Customer and Staffbase in an Order.

Employee App Privacy Policy. App Stores may require Customer to have a privacy policy in place when submitting the Employee App to the relevant App Stores. Customer is responsible for creating their own privacy policy. Staffbase shall use reasonable efforts to support Customer in creating the privacy policy, such as providing any needed documentation

or information about the functionality of the Employee App that is available to Staffbase. Customer shall not use, copy, or refer to a privacy policy created by Staffbase.

Employee App Privacy Labels. App Stores may require Customer to specify what user data is collected and shared by the Employee App, for example, via the creation of so called "privacy labels". Customer is responsible for answering any questions about the relevant Employee App data processing activities and for creating the appropriate privacy labels in accordance with an App Store's terms of service and requirements. Staffbase shall use reasonable efforts to support Customer, such as providing any needed documentation or information about the functionality of the Employee App that is available to Staffbase.

2. Front Door Intranet

Usage Limits. Front Door Intranet is licensed based on the number of Customer Personnel that are invited to access and use the Front Door Intranet (also deemed "**Invited Users**"). Staffbase will determine the Invited User count based on the data available in the Services. Deactivated Customer Personnel (previously Invited Users) who are no longer engaged or employed by Customer are not counted towards the total of Invited Users. For Customers using SSO integrations, including SCIM, SAML, or OIDC, without a regular sync with the Services of the full invited user base, the ability of Customer's Personnel to log in and register for the Front Door Intranet through the integration deems them an Invited User.

Custom Domains or Subdomains. Any Customer-provided names for any custom subdomains or custom domains related to their Front Door Intranet are "Customer Content" as defined in the Agreement. Customer owns all goodwill generated as a result of Staffbase's use of Customer's branding within custom subdomains or for custom domains (including any trademarks). Any changes to custom domains or subdomains after the initial selection has been made may be subject to additional fees, to be agreed between Customer and Staffbase in an Order Form.

3. Employee Email

Usage Limits. Staffbase's Employee Email product is licensed based on the number of contacts that are sent an email by Customer using the Employee Email product (**"Email Recipients"**). Where an email is sent to a distribution list, each unique contact on a distribution list is an Email Recipient. If Staffbase is unable to view the number of Email Recipients on a distribution list then Customer shall, on request, inform Staffbase of such number.

Staffbase Email for Outlook or Gmail Specific License. The following license terms apply in addition to the license permissions and restrictions in the Agreement. For Employee Email Staffbase grants Customer **(i)** where it downloads the Outlook add-on or Gmail extension, a worldwide, non-exclusive, non-transferrable, and non-sublicensable right and license during the Subscription Term to install and use the Outlook add-on or Gmail extension; and **(ii)** the right during the Subscription Term to distribute the Outlook add-on or Gmail extension, subject to Customer's compliance with any applicable terms and conditions of Outlook or Gmail. Upon any expiration or termination of a Subscription Term, Customer's license to use and distribute any software related to the Outlook add-on or Gmail extension terminates immediately.

Email tracking and analytics. Employee Email includes analytic features that enable Customer to analyze the success of email newsletters via advanced analytics and reports. To track email newsletter engagement, technologies like pixels and cookies may be used. Customer must determine whether Customer's use of these technologies is permitted under applicable law.

Customer's compliance with applicable law. Customer shall use Employee Email solely for Customer's internal communications and is responsible for any required consents, authorizations, or disclosures to Email Recipients as required by applicable law.

Customer's obligations to mitigate risks related to spam complaints. Email Recipients may have the option to mark Customer's emails as "spam". Customer understands that the Services may be impacted by the amount of spam complaints related to Customer's emails. Customer agrees that Staffbase may monitor spam complaints submitted by Email Recipients. Customer shall promptly follow Staffbase's instructions to mitigate any risks related to spam complaints in relation to Customer's use of the Services.

Customer Content. Customer acknowledges and agrees that any Customer Content that is part of an email newsletter, including media files, will be visible to each Email Recipient, and may be forwarded by an Email Recipient. Any additional access restrictions activated or implemented by Customer in relation to other Services are not applicable to media files contained in email newsletters sent via Employee Email. Customer is solely responsible for the configuration of lists of Email Recipients and Staffbase is not responsible for access to, or use of, email newsletters outside of the Services, such as email newsletters forwarded by Email Recipients.

4. Communications Control Platform

Usage Limits. The Communications Control Platform ("**Comms Control**") is licensed based on the number of users permitted to use Comms Control ("**Authorized Users**").

Storage space. Storage space for Comms Control is subject to limitations, as specified in the Dirico Documentation. Customer may be able to purchase additional storage space. Staffbase shall make available additional storage space as specified in the Order.

Customer's social media accounts. Comms Control allows Customer to send communication via various external channels, including Customer's social media accounts. Customer shall identify which third-party terms apply when connecting Comms Control to the relevant Customer's social media account. Customer shall comply with any applicable guidelines, terms and conditions, or policies of the relevant social media platform when using Comms Control. When Customer has connected its social media accounts to Comms Control, Staffbase may process Personal Data (as defined in the DPA) of individuals who engage with Customer via Customer's social media accounts (**"Social Media Contacts"**). Customer is responsible for any required consents, authorizations, and disclosures when processing Personal Data of Social Media Contacts in relation to Comms Control and when communicating with Social Media Contacts via Comms Control, as required by applicable laws and applicable social media terms and conditions. Staffbase is not responsible if a social media platform provider changes their API interface that results in a complete or partial use restriction of the relevant connection between the social media platform and Comms Control.

Security. Notwithstanding any other provision in the Agreement, the applicable technical and organizational measures in relation to Communications Control are currently available at: https://staffbase.com/en/legal/dpa/. Customer acknowledges that the technical and organizational measures applicable to Comms Control may differ from the technical and organizational measures that apply to other Services and that are described on Staffbase's security webpage, currently available at https://staffbase.com/en/security/.

Updated Definitions. When Customer uses Comm Control, the following definition applies:

"**Dirico Documentation**" includes the documentation available at https://helpcenter.dirico.io/en/articles/6911870-function-description.

5. AI Features

General. Certain features and functionality of the Services powered by artificial intelligence (including machine learning) (**"AI Features"**) allow Customer to provide prompts, scripts, queries or other input ("**Prompts**") in order to generate answers, text, images, or other content based on such Prompts ("**AI Output**"). As between the parties, and to the extent permitted by applicable law, Customer owns all AI Output. Customer shall ensure that its use of AI Features (including the use of any Prompts and AI Output) happens in a responsible manner and does not violate any applicable law or the Agreement.

Limitations to Generated Content. Customer acknowledges that there are limitations with respect to artificial intelligence (AI)-generated AI Output because it is automatically generated. AI Output may contain errors or be misleading, can be repetitive or formulaic, may be out of context or not make sense, and may be biased and generate content that is discriminatory or offensive.

Usage Limits. Staffbase may impose limits on the amount of AI Input that Customer can prompt or AI Output that Customer can create with Staffbase AI Products.

Personal Data Processing Instructions. If any Prompt includes Personal Data, Customer is deemed to be instructing Staffbase to process such Personal Data for the purposes of providing AI Output Otherwise, Staffbase shall only process such Personal Data in accordance with the applicable DPA.

Disclaimer. AI Outputs are generated through machine learning processes and are not tested, verified, endorsed or guaranteed to be accurate, complete or current by Staffbase. Customer should independently review and verify all AI Outputs as to appropriateness for any or all Customer use cases or applications.