

Acceptable Use Policy

Align's Acceptable Use Policy ("AUP") is designed to ensure compliance with all applicable laws and regulations governing the Align Managed Services Solution (the "Services"), and to promote the security and availability of client data to Align's clients ("Clients"). This AUP applies to each Client's use of the Services. This AUP applies to each Client's use of the Services including but not limited to Microsoft 365 configuration, administration, monitoring, ticketing, and cybersecurity services.

This AUP is incorporated, by reference, under the terms and conditions of the Master Agreement ("Agreement"). If there is a conflict between the Agreement or any SOW, on the one hand, and this AUP, on the other hand, the terms of this Agreement or the SOW, as applicable, will govern. Capitalized terms not defined herein have the meanings set forth in the Agreement. Align reserves the right to amend this AUP from time to time at its sole discretion. Clients will be notified of any modifications. Client's acceptance of any such amendments will be governed by the Agreement.

1. Scope and Responsibility Model

Align provides managed services related to the configuration, administration, monitoring, and support of Client-owned technology environments, including Client Microsoft 365 tenants (the "Client Environment"). Align does not host Client data, applications, or workloads. Client data resides within third-party platforms, including Microsoft, subject to those providers' terms.

Client remains solely responsible for the legality, accuracy, and appropriateness of all data, content, and communications within the Client Environment, as well as its user access, authorization, and compliance with applicable laws and regulations.

2. Client Responsibilities

Clients are responsible for complying with this AUP and for violations attributable to their users, whether authorized or not by the Client. Clients must take reasonable steps to ensure that their users will comply with this AUP. This AUP does not (a) obligate Align to monitor, review, or audit Client data and content transmitted by the Client or residing within the Service platform or (b) create any obligation of Align to any party that is not a Client.

3. Prohibited Use

Client shall not use, or permit users to use, the Services or Client Environment to violate applicable laws, transmit unlawful or harmful material, engage in fraud or misrepresentation, harass others, or compromise the confidentiality, integrity, or availability of systems or data. Clients shall be responsible for determining what laws or regulations are applicable to their use of the Services. A Client shall not knowingly use the Align Services to store or transmit any material believed by Client to constitute child pornography, torrents, gambling or any other illegal activity. In addition to the any other actions it may take under this AUP, Align reserves the right to cooperate fully with any criminal investigation of content located within the Align Services that constitutes alleged child pornography torrents, gambling or any other illegal activity.

4. Security Abuse

Clients shall not engage in activities that constitute security abuse, including but not limited to malware introduction, phishing, credential theft, unauthorized privilege escalation, abuse of administrative roles, intentional misconfiguration of security controls, or denial-of-service activity. Clients are prohibited from engaging in any activities that Align determines, in its sole discretion, to constitute security abuse, including the following:

- Introducing or executing malicious programs into the Service platform, such as viruses, worms, Trojan Horses, and key loggers.
- Causing or initiating security breaches or disruptions including but not limited to, port scans, flood pings, email-bombing, packet spoofing, IP spoofing, and forged routing information.
- Executing any form of malicious activity that will intercept data not intended for the Client's instance.
- Evading or circumventing user authentication or security of any account, including but not limited to, cracking, brute-force, or dictionary attacks.
- Interfering with or denying service to any user such as a denial of service attack or distributed denial of service attack.
- Using any program, or sending messages of any kind, designed to interfere with or disable a user's terminal session.

5. Client Security Obligations

Clients must use reasonable care to ensure compliance with this AUP. The Client is solely responsible for the actions of its employees or agents, that result in any intrusions into, or security breaches of its instance. Clients acknowledge that security incidents may arise from user behavior, compromised credentials, or third-party services outside Align's direct control.

6. Email, Messaging, and Collaboration

Client shall not use Microsoft 365 or related services to send unsolicited bulk messages in violation of anti-spam or privacy laws, forge sender identities, or operate unlawful mailing lists. To the extent required by law, Clients who send mass mailings must maintain complete and accurate records of all consents and opt-ins, including the actual e-mail and its headers.

7. Monitoring and Ticketing

Align may maintain operational logs, monitoring alerts, and ticketing records solely for service delivery, cybersecurity monitoring, incident response, and compliance purposes. Such records do not constitute ownership or control of Client data or content.

8. Legal Requests and Investigations

Client agrees to cooperate with lawful investigations relating to the Client Environment. Align may comply with lawful requests without notice where legally required and shall not be liable for service impacts resulting from such compliance. Align shall not be in default under any agreement for Services, if its compliance with any Investigation causes a Client to incur downtime or requires the sequestering of all or a portion of the Services.

9. Enforcement

Align may take reasonable actions to enforce this AUP, including restriction of administrative access, suspension of affected services, or termination of Services for material violations. No service credits shall be issued for interruptions caused by AUP violations. The aforementioned list of actions shall not be construed in any way to limit the actions or remedies that Align may take to enforce and ensure compliance with this AUP. Align reserves the right to recover any and all expenses and apply any reasonable charges in connection with a Client's violation of this AUP as and to the extent set forth in the Agreement. No service credits will be issued for any interruption in service resulting from violations of this AUP by the Client.

10. Disclaimer

CLIENT ACKNOWLEDGES THAT ALIGN DOES NOT HOST CLIENT DATA OR CONTROL THIRD-PARTY PLATFORMS, INCLUDING MICROSOFT. ALIGN IS NOT RESPONSIBLE FOR OUTAGES, DATA LOSS, OR SECURITY FAILURES ARISING FROM SUCH PLATFORMS, EXCEPT AS EXPRESSLY PROVIDED IN THE AGREEMENT.

ALIGN RESERVES THE RIGHT AT ALL TIMES TO INVESTIGATE ANY ACTUAL, SUSPECTED, OR ALLEGED VIOLATIONS OF THIS AUP, WITH SUCH INVESTIGATION TO INCLUDE ACCESSING OF DATA AND RECORDS ON, OR ASSOCIATED WITH, ANY SERVER.

Align

By: _____

Print Name: _____

Print Title: _____

Date Signed: _____

Customer

By: _____

Print Name: _____

Print Title: _____

Date Signed: _____