WEBFLOW INFORMATION SECURITY ADDENDUM

This Information Security Addendum ("***InfoSec Addendum***") is part of and hereby incorporated into the Master Subscription Agreement (the "***MSA***" and together with this and all other exhibits and Order Forms, the "***Agreement***") by and between Webflow, Inc. ("***Webflow***"), and the customer identified in the MSA or applicable Order Form incorporating the MSA ("***Customer***"). All capitalized terms used but not defined herein will have the respective meanings ascribed to them in the Agreement.

1. PURPOSE.

1.1. Scope. This InfoSec Addendum describes Webflow's information security program and infrastructure policies designed to protect Customer Data from unauthorized use, access, disclosure, theft, and/or manipulation (a "***Security Incident***") during the Subscription Term and any limited time thereafter during which Webflow has possession of or access to such Customer Data (e.g., Customer Data in backup systems that will be systematically purged in the usual course of business). For the avoidance of doubt, as the open nature of the Platform enables Customer to add or interconnect with content, assets, or services controlled or managed by Customer or third parties selected by Customer, this InfoSec Addendum does not apply to any such content, assets, or services.

1.2. Conflict. Notwithstanding any other term of the Agreement, in the event of a conflict or inconsistency between this InfoSec Addendum and the Agreement, the terms of this InfoSec Addendum shall control to the extent of such conflict.

2. PHYSICAL SECURITY.

2.1. Data Center. Webflow uses Amazon Web Services ("***AWS***") exclusively for the provisioning of data center facilities. The parties agree that AWS meets the physical security requirements appropriate for the processing and storage of Customer Data and Webflow regularly reviews the AWS certification of its data center facilities.

2.2. Webflow Offices. Webflow offices will not store tangible Customer Data in any form. Office facilities are protected with locks, cameras, and alarm systems.

2.3. Webflow Laptops. Notwithstanding Section 2.2 above, Customer Data may be temporarily downloaded onto Webflow-owned laptops for data analysis and/or troubleshooting. Laptops are security-hardened with a configuration that includes full-disk encryption, enforced password authentication, automatic screensaver with password unlock, and malware protection.

3. NETWORK, STORAGE, AND HOST SECURITY.

3.1. Transmission. Webflow will end-to-end encrypt Customer Data under Webflow's control traversing any public network using TLS 1.2 or better, and a cipher suite adhering to the recommendations of NIST SP 800-52.

3.2. Storage and Encryption. Webflow will store all Customer Data transmitted to Webflow in AWS S3 containers set with encryption-at-rest to AES256 or better; or in Webflow

databases encrypted to AES256 or better; or to online backups (i.e., system "snapshots") stored in AWS S3 containers set with encryption-at-rest. Decryption and management of encryption keys are controlled by Atlas MongoDB. Only NIST-approved ciphers and modes will be used for encryption.

3.3. **Storage Media**. Webflow will not store Customer Data on removable media (e.g., tapes, removable disks, flash drives, etc.) in the normal course of business. Except as expressly set forth herein, any transfer of Customer Data via removable media is prohibited without Customer's written approval.

3.4. **Intrusion Detection/Prevention**. Webflow will implement appropriate tools, equipment, and mechanisms in the environment of, and within, the application designed to reduce the risk of unauthorized access to Customer Data. Such tools may include deployment of firewalls, intrusion detection systems, malware detection, and malware interception software. Webflow will monitor all such tools, and assess and take steps necessary to address any incidents of which it becomes aware without undue delay.

3.5. **Web Application Firewall.** Webflow utilizes a Web Application Firewall (WAF) to detect certain kinds of brute-force attacks. Webflow monitors for increased traffic patterns that indicate DDoS attacks and has on-call staff 24/7/365 to respond within minutes when services are at risk of becoming overloaded beyond the ability of automated scaling measures.

3.6. **Production Segregation.** Webflow maintains separate demonstration, quality assurance, and test datasets that are used for the relevant environments and unrelated to real customer data.

3.7. **Virtual Private Cloud.** Webflow Platform is built on a serverless architecture in AWS and the architecture is based on the AWS global backbone. Webflow's VPC environment is architected with a 'Defense-in-Depth' security operations strategy, with numerous layers of security monitoring, protocols, and implementations protecting the confidentiality, integrity, and availability of the Webflow Platform application.

4. LOGGING AND MONITORING.

4.1. **Availability and Performance.** Webflow will monitor infrastructure, network, storage, and system performance on an ongoing basis.

4.2. **Security Alerts**. Webflow maintains intrusion detection systems that log events to the Webflow's Security team in real-time. Additional security logs are generated for periodic review by the Security team, including failed and successful login attempts. Log is accessible to designated Webflow Engineering and Security team, but logs are protected and may not be edited or modified.

4.3. **Log retention.** Webflow utilizes a SIEM tool to centrally manage audit logs. Webflow retains security logs for as long as necessary to provide the Platform and meet compliance obligations to Customer in accordance with the Agreement or for at least one year.

5. THIRD PARTY SECURITY.

5.1. **Vendor Due Diligence**. Webflow conducts appropriate due diligence prior to engaging any third party, vendor, subcontractor, or subprocessor used to provide any services to Webflow customers. Webflow requires its subprocessors to be bound by written agreements that include security, confidentiality, and privacy obligations appropriate to the services they provide and that are materially consistent with the commitments set forth in this Info Sec Addendum.

5.2. **Vendor Management**. Prior to granting any vendor access to any Webflow system or Customer Data, Webflow will evaluate all vendors to ensure their security controls are of a level consistent with or better than Webflow's own. Webflow uses a formal vendor risk management system based on recommendations in NIST SP 800-39.

5.3. **Vendor Certification and Warranty**. Webflow will evaluate and store vendor credentials, vendor engagement agreements, and any other artifacts as appropriate for the task engaged (such as PCI-DSS attestations for payment processors; ISO27001 for Infrastructure Providers; SOC-2 where applicable for SaaS, ISO 42001 for AI services providers) for at least one year past the lifetime of the vendor engagement with Webflow. Webflow will review such artifacts and credentials annually.

6. CUSTOMER ACCESS CONTROLS.

6.1. **Customer Authentication (SAML Login)**. Customers with Single Sign-On via the "Security Assertion Markup Language" standard can configure any access restrictions via Customer's IdP. All access controls (such as password complexity, multi-factor authentication, session length validity) are solely Customer's responsibility.

6.2. **Customer Authentication (OAuth2/SSO Login)**. Webflow customers with Single Sign-On via the "Open Authentication 2.0" or SAML 2.0 standards will either (a) allow users to configure any access restrictions via their OAuth2 or identity provider, or (b) may restrict domain access to an OAuth2/identity provider under their control (such as the enterprise GSuite, Okta, OneLogin, Ping identity, etc.). All access controls (such as password complexity or multi-factor authentication) are solely the responsibility of the IDP account holder. Where Customer controls the identity provider, all access controls are the responsibility of Customer. Webflow currently supports OAuth2 assertions from Google/GSuite, and SAML-based SSO from any SAML 2.0 compliant identity provider.

6.3. **Customer Authentication (username/password)**. Customers may enable username/password as a mechanism to authenticate users. Users self-register to the Platform. Customer passwords are stored within the Platform as hashes using industry standard techniques. Webflow does not store user passwords in the clear in any Webflow-controlled cache, file, database, or access log.

7. CUSTOMER DATA.

7.1. **Webflow Workspaces.** In the case of specific deletion to any workspace, Webflow will use commercially reasonable efforts to remove such Customer Data as promptly as practicable from shared access and the Platform following the completion of backup

cycles, as Customer Data may be temporarily retained in Platform backups after deletion.

7.2. **Access Control**. Webflow Platform's access controls will include commercially reasonable procedures to check and enforce access restrictions for network requests.

7.3. **Customer Data Segmentation**. Webflow will store Customer Data logically separate from data of its other customers. Assets that comprise a Webflow workspace are stored individually in encrypted AWS S3 containers, with the URL controlled by Webflow servers.

7.4. **Data Retention and Deletion.** Customer Data is retained only for as long as necessary to provide the Platform and meet compliance obligations. Upon request, Webflow provides Customer the option to delete Customer Data upon termination of the Agreement. Webflow shall delete Customer Data from currently running production systems within 30 days of Customer's deletion request.

8. INCIDENT MANAGEMENT.

8.1. **Assessment and Notification**. Webflow will promptly investigate all reported or detected security issues and assess the impact to Customer. If Customer is affected, Webflow will ensure Customer is notified within seventy-two (72) hours, to the email address provided by Customer for reporting security incidents (if any). The Security Incident notification will contain, at minimum, and to the extent such information is available: (i) a description of the Security Incident; (ii) any actions required from the Customer or impacted individual to mitigate harm; and (iii) the steps taken or planned by Webflow to investigate and mitigate potential harm. Webflow will reasonably cooperate with Customer to investigate and remediate the Security Incident and to assist Customer in mitigating any further risk.

8.2. **Remediation**. For any Security Incident that affects Customer, Webflow will inform Customer of the progress of any remediation periodically throughout the remediation activity. Depending on the nature of the Security Incident, Webflow will give Customer the opportunity to participate in the remediation. Upon written request, and within five (5) business days of the closure of the Security Incident, Webflow will provide Customer with a detailed report of the Security Incident (the "***Report***"). Customer shall treat such Report as Webflow's Confidential Information. Webflow will retain data related to the Security Incident for at least one year past the termination of this Agreement.

8.3. **Security Contact.** Customer may contact the Webflow Security team at security@webflow.com.

9. PLATFORM ACCESS CONTROLS.

9.1. **Authentication**. Webflow personnel will use individual credentials to access the Platform. All access permissions are role-based grants, on the principle of least privilege. Multifactor authentication is mandatory for system access. Additional multifactor authentication is required for access to core systems such as for infrastructure management or financial system access. Platform uses a VPN solution to

restrict authentication and access to restricted applications/systems by requiring authentication attempts to originate from an approved private network.

9.2. **Endpoint Devices**. The Platform's end-point devices will be configured to increase protection of any Customer Data that may be accessed, including full-disk encryption, mandatory login passwords, malware protection, a personal firewall, and password-secured screensavers.

9.3. **Limited Access.** Webflow will limit access to Customer Data to only those Webflow personnel that have a need to know in order to perform specific responsibilities related to providing the Platform to Customer. Webflow conducts formal quarterly user access reviews to ensure that each employee retains only the minimum permissions necessary for their role and to promptly remove or adjust access when no longer appropriate.

10. SOFTWARE DEVELOPMENT.

10.1. **Code Development**. Webflow uses a Secure Software Development Life Cycle (SSDLC) framework for all code development. All branches, features, and releases must be reviewed by more than one team member. Pull requests must be approved by an authorized team member. Automated code analysis and integration testing is applied before any code merge, and again before release to production.

10.2. **Change Management.** Webflow requires all code to pass all automated tests prior to being considered for release. A release must be approved by an authorized team member designated for that code area. Emergency fixes may be expedited but will still require approval from an authorized member of the responsible team. Incident management change control will be overseen by Webflow's security and privacy representatives.

10.3. **Software Frameworks**. Webflow uses industry-standard software frameworks and libraries: native HTML, and Javascript; Node.js on Backend. All frameworks are regularly reviewed for security issues and amendments made as appropriate to any deployed or in-development code.

10.4. **Threat and Vulnerability Management**. Webflow uses internal vulnerability scanning tools including AWS Inspector to identify known vulnerabilities in code. Webflow will undergo a penetration test carried out by an independent third party on at least an annual basis.

10.5. **Vulnerability Scans and Penetration Tests.** Webflow will perform annual penetration tests on Webflow's systems based on relevant identified risks and at least quarterly vulnerability assessments, including systematic scans or reviews of Webflow's systems, designed to identify publicly known security vulnerabilities based on the relevant identified risks. A high-level summary of the results of the penetration tests is available at https://trust.webflow.com/.

11. HUMAN RESOURCES SECURITY.

11.1. **Training**. All Webflow employees receive annual training on security and privacy requirements to comply with Webflow's information security policies and procedures.

Training is provided during employee onboarding and at least annually thereafter. All engineering staff members must also complete secure code training upon hire. Additional training is provided to address new threats as they emerge.

11.2. **Background Checks.** As required under Applicable Law and consistent with Webflow's then-current screening practices, Webflow will use commercially reasonable efforts to perform background checks on all Webflow personnel who will have access to Customer Data. To the extent permitted by applicable law, these background checks include: (i) verification of the personnel's identity and qualifications; (ii) confirmation of employment history; (iii) review of relevant criminal records; and (iv) review of credit reports for applicable positions. Webflow agrees not to knowingly assign any person to perform work under the Agreement who has been convicted of a violation of law involving injury to the public and resulting in jail or prison time, without Customer's express written consent.

12. BUSINESS CONTINUITY.

12.1. **Backup**. Webflow will maintain multiple snapshots of operational databases to be able to recover Customer Data. Backup restoration is restricted to Webflow Systems and Integration staff, and is authenticated by multifactor authentication. Snapshots will be encrypted to AES256 or better.

12.2. **Resiliency by Design**. Webflow will design backend servers to be naturally resilient. Single server failures will trigger automatic recovery/failover to another server for that function.

12.3. **Business Continuity**. Webflow will maintain business continuity plans that will allow full-service restoration in an alternative AWS region. Webflow will perform annual Business Continuity and Disaster Recovery Plan (BC/DRP) tests, Customer Data restoration times have a recovery point objective (RPO) of 4 hours and recovery time objective (RTO) of 24 hours.

12.4. **Disaster Recovery**. Webflow will maintain disaster recovery plans to recover from catastrophic impacts to the Platform and target full-service restoration at an alternative geographic location within the AWS infrastructure. Webflow will perform annual Business Continuity and Disaster Recovery Plan (BC/DRP) tests. Disaster Recovery Plans will ensure Customer Data has a RPO of 4 hours, and a RTO of 24 hours.

13. REGULATORY COMPLIANCE AND AUDIT.

13.1. **Security Attestation**. Webflow has implemented an information security management system to comply with the requirements of ISO 27001, ISO 27017, ISO 27018, PCI DSS security standards, and AICPA's SOC-2 program. Copies of Webflow's ISO certifications, PCI AOC, SOC 2 Type II reports will be available at https://trust.webflow.com/, or in the event that Webflow is still engaged in the process of obtaining such reports, as soon as reasonably possible.

13.2. **Audit**. Webflow will only seek accreditation or attestation from reputable auditors. Webflow will retain all audit results for at least two years. Customers may request the

results of audits. Customers do not have the right to independently audit Webflow or the Platform directly for any reason.