formstack

Last Updated July 2023

Formstack recognizes that the use of third party vendors creates various risks that must be properly managed. Before entering into any third party relationships, we take deliberate steps to conduct an assessment of risk related to the vendor relationship. We take care to understand the compliance, reputational, strategic, operational, and transactional risks relating to a particular vendor before entering into a contractual relationship.

Any vendor who has access to Formstack data classified as Confidential Information or higher, which includes Personal Information, are expected to demonstrate their security policies, processes, and procedures and prove that they are able to provide adequate protection of such data, including against misuse or compromise. The following sections outline the requirements (or substantively similar requirements) that vendors must follow if they collect, use or process Confidential Information or Personal Information while providing services or doing business with Formstack.

Organization of Information Security

Vendors must establish, implement, and maintain information security policies and a program of Technical and Organization Security Measures appropriate to prevent any access to Formstack Confidential Information and comply with and meet all applicable information security best practices standards and guidelines, including those set forth herein.

Secure Baseline Standards

Vendors must ensure that secure configurations are developed, documented, and maintained for information systems accessing Formstack Confidential Information. Baseline configurations must include software versions and security patch levels, managed anti-virus and malware detection, and must include security settings for audit and accountability.

Compliance and Accreditation

Vendors must be compliant with applicable laws, including regulatory laws, such as the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR) and should be able to support various security frameworks that Formstack deems fundamental in its operations when processing certain data, including the Payment Card Industry Data Security Standard (PCI-DSS) and Statement on Standards for Attestation Engagements 16 (SSAE16) Service Organization Controls (SOC) Type I or II.

Vendors may be asked to complete regular attestation audits, which evaluates internal controls and the Vendor’s information system relevant to security, availability, processing, integrity, confidentiality, and privacy.

Further to the above, Vendor must acknowledge and comply with export controls under the laws and regulations of the United States ("U.S.") and any other applicable jurisdictions, which govern export, re-export, import, transfer, distribution, and use of goods and services and shall obtain all required U.S. and any other applicable authorizations, permits, or licenses.

Vendors must maintain security related audits and certifications where Formstack Confidential Information is stored and must be able to attest to designated certifications. Vendor data centers or hosted colocations must have recently completed a Statement on Standards for Attestation Engagements 16 (SSAE16) Service Organization Controls (SOC) 2 audit or other certifications deemed adequate by Formstack. This report must be made available upon request. Vendors must have a process to document any non-compliance of any legal, regulatory or privacy instance or control that does not meet local laws and regulations and must identify and quantify the risks and mitigation plans and document the business decision for alternate controls or risk acceptance. The mitigation plan and business decision must be signed off by the Vendor Chief Information Officer (CIO) or an authorized individual who can accept responsibility and accountability.

Physical and Environmental Security

Vendor must ensure that all of Vendor’s systems and other resources intended for use by multiple users are located in secure physical facilities with access and authorization restrictions.

Vendor must ensure that all of Vendor’s employees, agents, third party vendors, or otherwise sign a non-disclosure or confidentiality agreement with Vendor prior to processing Formstack Confidential Information.

Vendor must limit and monitor physical access to its facilities to ensure that visitor access is logged and that access is restricted to appropriate personnel based on their job requirements. Vendors must require that all employees, contractors, and visitors present identification, log in, and be escorted by authorized staff through its facilities.

Access Control

Vendor must take all reasonable steps to prevent anyone from accessing Formstack Confidential Information in any manner or for any purpose not authorized by Formstack. Vendors must limit access to Formstack Confidential Information to Vendor’s employees, agents, and third party vendors who have a legitimate need to access Confidential Information to provide goods and/or services and have agreed in writing to protect the integrity, availability, and confidentiality of Formstack Confidential Information.

Vendors must maintain reasonable procedures to terminate access to Formstack Confidential Information when it is no longer needed or relevant to the performance of Vendor’s duties.

Vendors must separate Formstack information from any other customer’s or Vendor’s own applications and information either by using physically separate servers or alternatively by using logical access controls where physical separation of servers is not implemented.

Vendors must prohibit and employ reasonable Technical and Organizational Security Measures to ensure that any employee, contractor, or Vendor’s third party vendor processing Formstack Confidential Information may not copy, move, or store the Confidential Information onto any storage device.

Vendors must require at least two-factor authentication to remotely connect to internal Vendor resources containing Formstack Confidential Information.

Identification and Authentication

Vendors must assign unique user IDs to individual users and assign login credentials to one individual account. Vendors must have procedures for user account creation, timely account removal, and account modification (e.g., changes to privileges, span of access, functions/roles) for all access to Formstack Confidential Information and across all production, test, and development environments.

Vendors must require password complexity rules that at least meet the following password construction requirements: a minimum of eight (8) characters in length for system passwords and four (4) characters for tablet and smartphone passcodes. System passwords must contain three of the following: upper case, lower case, numeric, or special characters. Vendors must verify a user's identity and set one-time use and reset passwords to a unique value for each user after first use.

Passwords must not be the same as the user ID with which they are associated, contain a dictionary word, sequential or repeat numbers, and not be one of the last five passwords used. Vendors must also require password expiration at regular intervals and that all passwords are masked when displayed.

Failed login attempts must be limited to no more than five (5) failed logon attempts and lock the user account upon reaching that limit in a persistent state. Access to the user account can be reactivated subsequently through a manual process requiring verification of the user's identity.

System Security

Vendors must ensure that such systems and other resources are properly hardened in accordance with security best practices for establishing a secure information system baseline and including, but not limited to, removing or disabling unused network ports, protocols, and services, along with installing endpoint malware, antivirus, and host based firewall protection technologies.

Vendors must conduct internal vulnerability assessment scans including, but not limited to, networks, servers, applications and databases, with applicable industry-standard security vulnerability scanning software to uncover security vulnerabilities.

Vendors must use a documented process to apply appropriate security patches. Critical security vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 7.5 or higher must be installed immediately upon a patch or security update being made available and in no event longer than one month after release. Security vulnerabilities with a CVSS score of 4 or higher should be installed within 90 days of release.

Data Isolation and Segmentation

Vendors must implement a set of multi-layered security controls to logically isolate and segment Formstack Confidential Information in a hosted environment. Mechanisms to ensure appropriate isolation and segmentation must be implemented at the network, operating system, and application layers. Vendors must ensure that clients in a hosted environment are isolated from each other such that they are considered to be separately managed entities with no connectivity between them. Any system or component shared by the client environments, including but not limited to hypervisors and underlying infrastructure systems must not provide an access path between these environments.

API Integration

Use of an application programming interface (API) must be secured through a combination of methods that include the Strong Encryption of data being transmitted as part of the API call, using the latest supported versions of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections to during transmission, and implementing authentication and session management correctly by using secure procedures to create, manage, and end a session for each authorized user.

Auditing and Monitoring

Vendors must maintain an automated audit trail that documents system security events as well as any change management event that results in the access, modification, and/or deletion of Formstack Confidential Information.

The audit trail should, at a minimum, record the following information for each event:

- Type of event occurred
- Date and timestamp of when the event occurred
- The source of the event
- The outcome (success or failure) of the event
- The identity of any user/subject associated with the event

Audit logs must be read-only and protected from unauthorized access. Audit records documenting events resulting in the access, modification, and/or deletion of Formstack Confidential Information must be made available to Formstack

Vendors must employ a regular audit log review process (either manually or automated) for detection of unauthorized access to Formstack Confidential Information.

Network Security

Vendors must maintain a formal process for approving, testing, and documenting all network connections and changes to the firewall and router configurations. Vendors must configure firewalls to deny and log suspicious packets, and restrict network connections that only allow appropriate and authorized traffic, denying all other traffic through the firewall. Firewall rules must be reviewed on a recurring basis.

Vendors must restrict unauthorized outbound traffic from applications processing, storing or transmitting Formstack Confidential Information to IP addresses within the Demilitarized Zone DMZ and Internet.

When using radio frequency (RF) based wireless networking technologies to perform or support services and products for Formstack, vendors must ensure that any Formstack information transmitted is protected using appropriate encryption technologies sufficient to protect the Formstack information. Wireless technologies must use Strong Encryption, and Vendors must regularly scan, identify, and disable unauthorized wireless access points.

Data Protection, Sanitization, and Destruction

Vendors must use Strong Encryption for the transfer of Formstack Confidential Information outside of Vendor controlled networks or when transmitting Formstack Confidential Information over any untrusted network.

Vendors must use Strong Encryption to protect Formstack Confidential Information when stored. Vendor must not store Formstack Confidential Information electronically outside of Vendor’s network environment unless the storage device (e.g., backup tape, laptop, memory stick, computer disk, etc.) is protected by Strong Encryption.

Vendors must not store Formstack Confidential Information on removable media (e.g., USB flash drives, thumb drives, memory sticks, tapes, CDs, or external hard drives) except: (a) for backup, business continuity, disaster recovery, and data interchange purposes as allowed and required under the Agreement and (b) using Strong Encryption.

Upon termination of the Agreement or at any time prior to reuse or repurposing of media used to store or process Formstack Confidential Information, media must be cleared or purged in accordance with NIST SP 800-88. If the media is to be destroyed, Vendor must provide a certificate of destruction to Formstack upon request. Prior to such destruction, Vendor must maintain all applicable Technical and Organizational Security Measures to protect the security, privacy and confidentiality of Formstack Confidential Information.

Incident Response and Notification

Vendors must maintain a current Incident Management Process and must notify Formstack without undue delay after becoming aware of any potential destruction, loss, alterations, unauthorized disclosure of, or access to or accidental or actual destruction, loss, alteration, unauthorized disclosure of, or access to Formstack Confidential Information, including data, transmitted, stored or otherwise processed by the Vendor or its sub-processors.

Vendors must have and use an Incident Management Process that is managed by trained resources. The Vendor Incident Management Process must be consistent with various state and federal laws and regulatory requirements as well as published best industry compliance and governance standards.

Vendors must follow incident response best practices and make reasonable efforts to identify the cause of incidents and take appropriate steps in order to remediate the cause of the incident.

Under no circumstances shall Vendor publicly disclose any such breach of Formstack information, systems, or other resources. Vendor must immediately notify Formstack of a possible or actual incident and work directly with Formstack, as requested by Formstack, to notify applicable government officials, authorities, credit monitoring services, individuals affected by such breach, and/or any applicable media outlets, as required by law.

Business Continuity Management and Disaster Recovery

Vendors must develop, operate, manage, and revise business continuity and disaster recovery (BCP/DR) plans. Such plans must include BCP/DR roles and responsibilities, established recovery time objectives and recovery point objectives, daily back-up of data and systems, off-site storage of backup media and records, record protection and contingency plans commensurate with the requirements of the Agreement. Vendors must securely store such plans off-site and ensure such plans are available to Vendor as needed.

Vendors must have documented procedures for the secure backup and recovery of Formstack Personal Data or higher, which must include, at a minimum, procedures for the transport, storage, and disposal of the backup copies of the data and, upon Formstack' request, provide such documented procedures.

Definitions

"Agreement" means the contract or other legal document entered by Formstack and the Vendor.

“Affiliates” shall mean, with reference to a party, any company or other legal entity which: (i) controls either directly or indirectly, a party; or (ii) is controlled, directly or indirectly, by a party; or (iii) is directly or indirectly controlled by a company or entity which directly or indirectly controls a party. For these purposes, “control” means the right to exercise more than fifty percent (50%) of the voting or similar right of ownership; but only for so long as such control shall continue to exist.

“Confidential Information” means any commercially sensitive, proprietary or otherwise Confidential Information relating to Formstack, its Affiliates or the contents and/or purpose of the Agreement, whether oral, in writing or which by any other means may directly or indirectly come into the Vendor’s possession or into the possession of a Vendor personnel or the Vendor’s personnel, agents, contractors or sub-contractors as a result of or in connection with the Agreement. For the avoidance of doubt, all work product shall constitute Confidential Information.

“Incident Management Process” is a Vendor-developed and documented process and procedure to be followed in the event of an actual or suspected attack upon, intrusion upon, unauthorized access to, loss of, or other breach involving the confidentiality, availability, or integrity of Formstack Confidential Information.

“Personal Information” as defined under European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) as and other applicable global information security, data protection, and privacy laws, means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Examples include, but are not limited to: full name (including prefix and suffix), personal identification number (PIN) or password, payment card information or associated numbers (e.g. CVV number), bank account information, email addresses, phone number, physical address, information evidencing health status (e.g. prior treatments) or health requirements, travel documents such as driver’s license number, state or national ID number, passport number, citizenship, residency, date of birth, sexual orientation, religion, trade union membership, social security number or visa number, criminal history, biometric or genetic data.

“Strong Authentication” means the use of authentication mechanisms and authentication methodologies stronger than the passwords required herein. Examples of Strong Authentication mechanisms and methodologies include digital certificates, two-factor authentication, and one-time passwords.

“Strong Encryption” means the use of encryption technologies with minimum key lengths of 256-bits for symmetric encryption and 1024-bits for asymmetric encryption whose strength provides reasonable assurance that it must protect the encrypted information from unauthorized access and is adequate to protect the confidentiality and privacy of the encrypted information, and which incorporates a documented policy for the management of the encryption keys and associated processes adequate to protect the confidentiality and privacy of the keys and passwords used as inputs to the encryption algorithm. Strong Encryption includes, but is not limited to: SSL v3.0+/TLS v1.0+, Point to Point Tunneling Protocol (PPTP), AES 256, FIPS 140-2 (United States government only), RSA 1024 bit, SHA1/SHA2/SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric v4, or WPA2.

“Technical and Organizational Security Measures” mean any activities required under these Information Security Requirements to access, manage, transfer, process, store, retain, and destroy information or data; to disclose and notify affected parties required under the Agreement and under applicable information privacy and data protection laws; and to safeguard information or data to ensure availability, integrity, confidentiality, and privacy, or notify individuals of any failure to safeguard such information or data. Measures include but are not limited to those required or interpreted to be required under European Union General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) as promulgated under member countries, the United States Gramm-Leach Bliley Act (GLBA), the United States Health Insurance Portability and Accountability Act (HIPAA), and any other international and U.S. laws, official legal interpretation, or case precedent pertaining to information or data under the Agreement.

“Vendor” means the contracting entity set forth in the Agreement together with its Affiliates.