MojoHost Technical and Organizational Measures

Last Updated: March 25, 2022

MojoHost is responsible for the security measures set out in the Agreement and, in addition, will maintain and implement the following technical and organizational measures concerning the security of the Customer Configuration.

A. Physical Security.

Reference	**Physical Security - Control Description**
A.1. **Policy**	MojoHost will maintain a formal physical and environmental security program for any MojoHost operated facilities used to perform the Services.
A.2. **Access**	Visitors to MojoHost facilities used to perform the Services will be required to check in with reception/security before being granted access to MojoHost facilities. The visitor log will be compiled and reviewed in the event of an incident. Visitors without a government-issued ID will be denied access to MojoHost facilities used to perform the Services. Visitor badges are used to identify visitors at MojoHost facilities.
A.3. **Security**	Controlled building access and secure access to specific areas of MojoHost operated facilities used to perform the Services will be enforced through the administration of proximity-based access cards and biometric hand scanners or other approved security authentication methods. MojoHost will use proximity cards at its facilities used to provide Services to secure access to buildings and sensitive areas appropriately. Physical access is disabled within the timeframe specified by a maintained access termination standard when physical access is no longer needed due to termination of employment or Services. To effectively manage physical security incidents, an incident response process has been instituted to respond to, and document physical security incidents at MojoHost operated facilities used to perform the Services.

B. System Security.

B.1. Access Controls.

Reference	**Access Controls - Control Description**
B.1.1. *Access & Bastions*	For Hosted Systems: MojoHost's access to the Customer Hosted System and Customer VLANs will occur through dedicated bastion servers designed for this purpose, and MojoHost employees will authenticate with the bastion server using a dedicated user ID (including the assigned corporate SSO credential) and a two-factor authentication mechanism. For Customer Configurations other than Hosted Systems: MojoHost's access to the control panel permitting access to the Customer Configuration will require

Reference	Access Controls - Control Description
	two-factor authentication, will be managed through MojoHost's LDAP Active Directory group, and will be limited to support personnel and those ancillary services teams at MojoHost who require that access to provide or support the Services. Network security group rules are maintained on the Customer Configuration subnets to allow access over established RDP and SSH ports for remote administration. In addition, the Customer Configuration bastion subnet is locked down to only allow remote access from the MojoHost Support Bastions. MojoHost manages and leverages local server users, tied back to established corporate identities. Server authentication requests are directed to a known MojoHost ADFS endpoint for dual-factor authentication. As part of the user authentication flow, local user accounts are only enabled when an authenticated access request is granted and are constrained to the requested device. The MojoHost support team maintains a list of approved technicians who can execute the user access workflow.
B.1.2. *Access Review*	MojoHost will maintain a formal program to review access to the Customer Configuration by any MojoHost employee ("**Access Review Program**"). This does not include additional logging at the server or device or instance level (which a customer can enable at their option or request assistance as part of the Services). The Access Review Program is designed to ensure that no active IDs or accounts exist that are not linked to one or more MojoHost Personnel; IDs, or accounts for terminated MojoHost Personnel are deleted as appropriate; and that MojoHost is complying with its access provisioning process.
B.1.3. *Remote Access*	MojoHost personnel may use a Virtual Private Network (VPN) utilizing two-factor authentication (RSA token and password) to connect remotely to MojoHost networks. Once inside the MojoHost network, support staff members are required to go through a second level of authentication through the MojoHost Support Bastion/jump hosts/gateway servers to access Customer Configurations.
B.1.4. *Password Policy*	MojoHost will maintain a formal policy concerning the requirements for password and authentication regarding MojoHost's access to Customer Configurations and the MojoHost Shared Infrastructure ("**Password Policy**"). The Password Policy will provide for a secure method of assigning and selecting passwords or require the use of unique identifier technologies (e.g., biometrics or token devices); require control of data security passwords to ensure that those passwords are kept in a location or format that does not compromise the security of the data they protect; require MojoHost to prevent or limit users from further access after a number of unsuccessful attempts to gain access; ensure that access to each user account relating to the MojoHost Shared Infrastructure meets: (a) the authentication requirements set out in the Agreement and (b) if and to the extent not otherwise set out in the Agreement, industry standards (two-factor authentication when accessing MojoHost Shared Infrastructure from the Internet); and ensure that all MojoHost managed computing devices will be configured to lock (i.e. prevent access to the computing device) after a period of

Reference	Access Controls - Control Description
	inactivity (which period of inactivity will be no longer than 15 minutes or the applicable period set out in the Agreement) requiring users of the applicable computing device to enter their credentials to regain access to the computing device.
B.1.5. *Encryption or Pseudonymization*	Customer may employ encryption of data stored within the Customer Configuration by electing to purchase or use capabilities provided by MojoHost or otherwise obtained by Customer from nonparties.

B.2. Vulnerability Assessments.

Reference	Vulnerability Assessments - Control Description
B.2.1. *Customer Testing*	Subject to MojoHost's written consent (for Hosted Systems) or agreement of any applicable Third-Party Cloud provider (for Third-Party Cloud infrastructure), Customer may perform network and application security scans that tests the Customer Configuration for one or more of the following: (a) security vulnerabilities, (b) denial of service vulnerabilities, (c) system access, and (d) other intrusive activities including password cracking. Unless identified in the Service Order, the Services do not include support for those activities. If, as a result of those activities, Customer identifies any vulnerabilities on the MojoHost Shared Infrastructure, MojoHost will correct any discovered vulnerabilities on MojoHost Shared Infrastructure within a reasonable timeframe or as otherwise required by the Agreement.
B.2.2. *Monitoring, AoC*	MojoHost will perform ongoing monitoring and testing of the MojoHost Shared Infrastructure (to include vulnerability scanning, scheduled penetration testing, and maintenance) under applicable PCI standards and applicable MojoHost Policies and Standards ("**Vulnerability Assessments**"). MojoHost will make available its Attestation of Compliance to Customer on an annual basis.

B.3. System Defense.

Reference	System Defense - Control Description
B.3.1. *General*	MojoHost will: (a) use reasonable current security measures (including IDS/IPS/virus and malware scanning/cryptographic and key management processes) designed to protect the MojoHost Shared Infrastructure; (b) secure web servers used by MojoHost to provide the Services and the MojoHost customer portal to reduce the risk of infiltration, access penetration by, or exposure to, a nonparty by (i) protecting against intrusions, (ii) securing those servers, and (iii) protecting against intrusions of operating system software, in each case under the MojoHost Policies and Standards; (c) maintain patching practices for MojoHost Shared Infrastructure under the MojoHost Policies and Standards; and (d) maintain current firewalls around the MojoHost Shared

Reference	System Defense - Control Description
	Infrastructure and provide general maintenance and monitoring of those firewalls and active 24/7 monitoring of those firewalls to identify attempted unauthorized access to the MojoHost Shared Infrastructure.
B.3.2. *DDoS Mitigation*	MojoHost will use several tools to detect and trace network-wide anomalies, including denial-of-service (DoS) attacks and worms against the MojoHost Shared Infrastructure. Access control lists (ACLs) are used on Internet edge routers to mitigate distributed denial of service (DDoS) attacks against the MojoHost Shared Infrastructure. Through network-wide, router-based sampling, MojoHost will evaluate existing, and potential threats by aggregating traffic from across the MojoHost Shared Infrastructure. To help maintain the integrity of the MojoHost Shared Infrastructure and prevent disruption to support operations, MojoHost will continuously monitor connectivity and performance for multiple bandwidth providers, including routers and switches. MojoHost will use fully redundant routing and switching equipment for its core networking infrastructure elements of the MojoHost Shared Infrastructure.
B.3.3. *Separation*	MojoHost will use logically separate networks (vLANs) for internal traffic, administering customer environments from specified networks within the MojoHost Shared Infrastructure.
B.3.4. *Role-Based Access Controls*	MojoHost will secure access to core networking infrastructure elements of the MojoHost Shared Infrastructure using the inherent access control functionality in TACACS+/ACS software (or equivalent). Administrator access to network devices supporting MojoHost Shared Infrastructure is limited to authorized MojoHost Personnel. New administrator access to network devices supporting MojoHost infrastructure is granted through a maintained new user creation process. Access is role-based, and deviations require managerial approval. TACACS+/ACS (or equivalent) access lists are reviewed periodically to verify that those users on the list still require access to network devices. Any discrepancies found are corrected.
B.3.5. *Security Services*	MojoHost will provide a firewall, IDS, and any other security devices in Customer's dedicated Hosted System only if Customer purchases those devices and then under the applicable Product Terms for those devices.
B.3.6. *MojoHost Support Bastion Security*	MojoHost will maintain a formal program to ensure that the MojoHost Support Bastions used to access the Customer Configuration have malicious software protections in place, are maintained in good technical working order, are regularly scanned for vulnerabilities, and are patched with the latest applicable software updates.
B.3.7. *Policy, Demarcation*	MojoHost will maintain a formal program for securing access to the MojoHost Shared Infrastructure and ensure all access points and boundaries to MojoHost's network are clearly documented and protections against unauthorized access are implemented.

C. Incident Response.

Reference	Incident Response - Control Description
C.1. **Notification**	MojoHost will report to Customer as soon as reasonably practicable in writing and in accordance with law, of a material breach of the Customer Configuration security that results in unauthorized access to Customer Data resulting in the destruction, loss, unauthorized disclosure, or alteration of Customer Data of which MojoHost becomes aware. On request, MojoHost will promptly provide to Customer all relevant information and documentation that MojoHost has available regarding the Customer Configuration for any security incident. MojoHost is not obligated to notify routine security alerts concerning the Customer Configuration (including pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing, or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers, or similar incidents) except as otherwise specifically set out in the Agreement. MojoHost will follow standard incident procedures defined in MojoHost's Policies and Standards.
C.2. **Policy**	MojoHost responds to security incidents identified on the MojoHost Shared Infrastructure with a defined process to rate and remediate those incidents within reasonable timeframes depending on the severity of the incident and maintains a documented process to report, evaluate, and respond to security incidents ("**Management of Information Security Incidents Policy**").

D. Personnel Controls.

Reference	Personnel Controls - Control Description
D.1. **Screening**	MojoHost will screen individuals with access to organizational information systems when the role or position of those individuals with MojoHost provides access to Customer Data and as otherwise required by the Agreement. MojoHost will conduct the appropriate level of background screening required by ISO/PCI-DSS, as applicable to MojoHost. MojoHost will maintain documentation that validates that MojoHost has completed the appropriate level of screening requirements. MojoHost will maintain and follow a written procedure for how MojoHost will comply with the screening and requirements, which will be available for review by Customer on request.
D.2. **Removal**	If an employee satisfies the screening requirements, but MojoHost later becomes aware of any information that would result in an employee failing any of the screening requirements, MojoHost will promptly suspend or remove the employee's access to Customer Data and prohibit the employee from performing any Services for Customer involving access to Customer Data in accordance with any requirements under the Agreement.

Reference	Personnel Controls - Control Description
D.3. **Policy**	MojoHost will maintain documented and monitored procedures that define appropriate IT security-related roles and responsibilities for MojoHost Personnel; ensure that MojoHost Personnel have access only to the systems they have a business need and authorization to use; prohibit the copying of Customer Data to any portable physical device of any kind for access of Sensitive Data outside of a MojoHost controlled access facility; identify an owner for critical systems and responsibilities for key tasks and assign those tasks to individuals capable of performing them as they relate to the MojoHost Shared Infrastructure; include security responsibilities and confidentiality provisions within MojoHost employees' terms of employment; retain documentation of security awareness training, confirming the completion of this training for each member of MojoHost Personnel engaged in providing the Services requiring access to Customer Data; control the creation, change, and termination of MojoHost Personnel user accounts; and maintain a disciplinary process for policy violations.
D.4. **Awareness**	As part of implementing and ongoing support for information security policies, all MojoHost Personnel are required to participate in training and awareness sessions to support the importance of security within MojoHost's organization. MojoHost will maintain an ongoing security awareness program for employees to provide updated guidance and practice information on (a) securing data and assets and (b) threat reports. MojoHost will release regular notifications to employees focusing on prominent security issues.
D.5. **Competence**	MojoHost will maintain 24/7 staffing to support MojoHost Shared Infrastructure systems critical to MojoHost's performance of the Services under the Agreement, including staffing support and data center operations teams with technicians certified in various areas of expertise.
D.6. **Hiring**	MojoHost will base hiring decisions on factors relevant to the performance of MojoHost's obligations under its customer agreements, including evaluating educational background, prior relevant experience, past accomplishments, and evidence of integrity and ethical behavior.

E. Data Center Controls – MojoHost Shared Infrastructure.

Reference	Data Center Controls - Control Description
E.1. **Environmental Controls**	MojoHost Shared Infrastructure data center facilities are equipped with redundant HVAC units to maintain consistent temperature and humidity levels. MojoHost Shared Infrastructure HVAC systems are inspected regularly, and air filters are changed as needed. Redundant lines of communication exist within the MojoHost Shared Infrastructure to telecommunication providers providing MojoHost customers with failover communication paths in the event of data

Reference	Data Center Controls - Control Description
	communications interruption. MojoHost Shared Infrastructure data centers are equipped with sensors to detect environmental hazards, including smoke detectors and floor water detectors. MojoHost Shared Infrastructure data centers are also equipped with raised flooring to protect hardware and communications equipment from water damage. MojoHost Shared Infrastructure data centers are equipped with fire detection and suppression systems and fire extinguishers. Fire detection systems, sprinkler systems, and chemical fire extinguishers MojoHost Shared Infrastructure are inspected annually. MojoHost Shared Infrastructure data center facilities are equipped with uninterruptible power supplies (UPS) to mitigate the risk of short-term utility power failures and fluctuations. The MojoHost Shared Infrastructure UPS power subsystem is at least N+1 redundant with instantaneous failover in the event of a primary UPS failure. The MojoHost Shared Infrastructure UPS systems are inspected or serviced or both at least annually. MojoHost Shared Infrastructure data center facilities are equipped with diesel generators to mitigate the risk of long-term utility power failures and fluctuations. MojoHost Shared Infrastructure generators are tested at least every 120 days internally and tested at least annually by a third-party contractor to maintain proper operability in the event of an emergency.
E.2. **Physical Controls**	MojoHost Personnel are on duty at MojoHost operated data center facilities 24 hours a day, seven days a week. MojoHost Personnel are required to display their identity badges at all times when onsite at MojoHost facilities. Two-factor authentication is used to gain access to the server room floors of MojoHost Shared Infrastructure. Electromechanical locks within MojoHost Shared Infrastructure are controlled by biometric authentication (e.g., biometric scanner) and keycard/badge. Only authorized personnel have access to MojoHost operated data center facilities. Closed-circuit video surveillance has been installed at entrance points on the interior and exterior of the buildings housing MojoHost operated data centers and is monitored by authorized personnel. The CCTV retention period is at least 90 days.

F. Media Protection – Hosted Systems.

Reference	Media Protection - Control Description
F.1. **Single-Pass**	MojoHost will zero-fill (meaning to format the hard disk drive by filling available sectors with zeroes) any hard disk drive dedicated to Customer’s use as part of a Hosted System before re-using the hard disk drive in an MojoHost data center.
F.2. **Physical Destruction**	On Customer’s written request, MojoHost will destroy (by hole punch, degaussing, or other mechanisms) any media dedicated to Customer’s use as part of a Hosted System, and MojoHost will provide documentation or certification to Customer of that destruction. MojoHost may charge Customer a fee for those Services at its then-current rates as applicable.

Reference	Media Protection - Control Description
F.3. **Multi-Pass**	Customer may designate the hard drives dedicated to Customer's use as part of a Hosted System as requiring a three-pass wipe (on failure as possible, or on replacement or cancellation) on written notice to the MojoHost account manager. MojoHost will perform a three-pass wipe on that media on a failure, replacement, or cancellation event, and Customer will reimburse MojoHost at MojoHost's then-current rates for those Services.
F.4. **Geographic** **F.5.** **Control**	Except in the case of a consolidation of MojoHost data center facilities or as otherwise specifically stated in the Agreement, MojoHost will not relocate the Customer's Hosted System from a MojoHost data center in one country to another without Customer's express written permission. The parties acknowledge that off-site backup involves transporting encrypted media containing Customer Data to a third-party site.

G. Risk Assessment Controls.

Reference	Risk Assessment Controls - Control Description
G.1. **Policy**	MojoHost will incorporate risk management throughout its business operations. MojoHost will conduct internal information security risk assessments regarding MojoHost Shared Infrastructure.
G.2. **Oversight**	MojoHost will manage identified risks to the MojoHost Shared Infrastructure on an ongoing basis through formal project management processes, provide an overall strategic plan, and operationalize that plan.
G.3. **Review**	MojoHost will assign managerial and supervisory personnel to be responsible for monitoring the quality of internal MojoHost Shared Infrastructure security control performance as a routine part of their job responsibilities. MojoHost's management will review key reports to verify appropriate actions have been taken.
G.4. **Assessments**	MojoHost will undertake security risk assessments per the MojoHost Policies and Standards regarding MojoHost Shared Infrastructure and MojoHost corporate networks. The risk assessment includes: (a) identifying and assessing reasonably foreseeable internal and external threats and risks to the privacy, confidentiality, security, integrity, and availability of personal information; (b) assessing the likelihood of, and potential damage that can be caused by, identified threats and risks; (c) assessing the adequacy of and compliance with personnel training concerning MojoHost's information security program; (d) assessing the adequacy of service provider arrangements; (e) adjusting and updating MojoHost's information systems and information security program to limit and mitigate identified threats and risks and to address material changes in relevant technology, business practices, personal information practices, and sensitivity of personal information that MojoHost processes; and (f) assessing whether

Reference	Risk Assessment Controls - Control Description
	MojoHost's information security program is operating in a manner reasonably calculated to prevent and mitigate information security incidents.

H. Change & Configuration Management Controls.

Reference	Change & Configuration Management Controls - Control Description
H.1. **Process**	MojoHost will cooperate in good faith with Customer to create a run book or account management guidelines ("**Run Book**"), which will contain the controls applicable to system or network changes and detail the system or change management process as agreed on with Customer. MojoHost will provide Customer with a mechanism to apply patches to the Hosted System and apply patches at Customer's request, as stipulated in the Run Book.
H.2. **Run Book**	MojoHost will make the Run Book and any attendant documentation available to Customer promptly on Customer's request, will update the Run Book with any reasonable process management controls for the Customer Configuration requested by Customer, and will otherwise cooperate with Customer in good faith to review or implement those system/network change management processes for the Customer Configuration as Customer requests.
H.3. **Windows**	MojoHost will maintain change windows for implementing or completing system/network changes to the Customer Configuration that comply with any change window requirements in the Agreement.
H.4. **Approval, History**	Customer is required to approve material changes to be made by MojoHost to the Customer Configuration before the change is implemented, except in the cases of predefined proactive MojoHost Shared Infrastructure maintenances, urgent security patches and fixes, downtime events where Customer cannot be reached (or has provided prior approval for action), and emergency maintenances (in which case MojoHost will provide Customer with reasonable notice of that change activity). The ticket history associated with the MojoHost account will be available for review through the MojoHost customer portal, thus providing a history of changes to the Customer Configuration performed by the MojoHost support team.

I. Business Continuity Planning.

Reference	Business Continuity Planning - Control Description
I.1. **Policy**	MojoHost maintains an Information Security Aspects of Business Continuity Policy that includes defined requirements for information security and continuity of information security management for MojoHost Shared Infrastructure during MojoHost business recovery events; defined management structure to prepare for, mitigate, and respond to a MojoHost business recovery

Reference	Business Continuity Planning - Control Description
	event involving MojoHost Shared Infrastructure using personnel with the necessary authority, experience, and competence; and verification, review, and testing of defined information security continuity controls related to the MojoHost Shared Infrastructure regularly.
I.2. **BCP**	MojoHost maintains an internal business continuity plan designed to permit MojoHost to resume its business operations after an interruption ("**Business Continuity Plan**"). This Business Continuity Plan does not cover Customer Configuration directly (is no substitute for redundancy or data backup, and in no way guarantees the restoration of the Customer Configuration or any Customer Data in the event of severe business interruption).