KERNSHELL

Kernshell Security Standards

These Security Standards describe the information security program adopted by Kernshell to help secure Customer Data against unauthorized processing and accidental or unlawful loss, access, or disclosure (the "Information Security Program"). These Security Standards are in addition to and not in lieu of any additional security requirements specified in any agreements between Kernshell and Customer. These Security Standards apply to Customer's use of the Services by Customer under the terms of the Kernshell Master Subscription Agreement (the "Agreement") between KERNSHELL TECHNOLOGIES PRIVATE LIMITED ("Kernshell") and the Customer that is a party to the Agreement and is incorporated into the Agreement by reference. These Security Standards apply separately to each account using the Services. Capitalized terms will have the meaning specified in the Agreement. We reserve the right to change the terms of these Security Standards at any time by posting a revised version at https://www.kernshell.com/terms-of-service/.

Effective Date: 02-April-2021

1. **Policies.** Kernshell will adopt and apply information security policies derived from applicable industry standards. Currently, Kernshell's policies are derived from the National Institute of Standards and Technology (NIST) Risk Management Framework. Such policies shall address adoption of managerial, operational, and technical security controls designed to help protect the confidentiality, integrity, and availability of Customer Data. Policies will be periodically reviewed to determine whether different or additional security measures are required to respond to new security risks or findings generated by the reviews.

2. **Data Storage.** Customer Data is stored at independently verified SSAE-16 / SOC I Type II certified Tier-III data centers. The data centers' physical and environmental security includes network hardening and active monitoring, digital security video surveillance, 24/365 on-site security staff, and biometric access control.

3. **Role-Based Logical Access Control.** Kernshell will maintain role-based access controls and policies to manage what access is allowed to the Kernshell Network, including the use of firewalls or functionally equivalent technology and authentication controls. Kernshell employs role-based access controls to servers containing Customer Data. Authorized personnel must use individual account and authentication credentials to gain access to Customer Data. Kernshell controls access to back-end servers through authentication handled with key-based SSH sessions.

4. **Security Awareness Training.** Kernshell requires security awareness training for personnel with access to Customer Data.

5. **Secure Data Transfer.** Kernshell requires that all Customer Data transmitted to or from the Kernshell Network use approved secure transfer processes such as secure file transfer protocol (SFTP). Data traversing the SFTP connection is authenticated and encrypted during transmission utilizing public/private keys.

6. **Network and Security Monitoring.** Kernshell's infrastructure incorporates firewalls, intrusion detection systems, vulnerability management tools and other technologies designed to monitor for network security events.

7. **Vulnerability Assessments.** Kernshell performs periodic internal and external vulnerability assessments of the Kernshell Network and Web Applications that include the use of independent third-party assessors as part of its ongoing monitoring program to assess the application and operation of its security controls. The scope of these audits includes assessment of compliance with Open Web Application Security Project (OWASP) Top 10 Web Vulnerabilities (www.owasp.org).

8. **Web Application Security Controls and Procedures:**

   Kernshell's web applications provided as part of the Services (the "Web Applications") employ the following controls and procedures,

   8.1. Secure Web Communications. Use of HTTPS for securing web server to web browser communications using a transportation layer security (TLS) encrypted - 2048 bit certificate signed by an approved certificate authority.

   8.2. User Authentication. Access requires a valid unique user ID and password combination, which are encrypted while in transmission.

   8.3. Security Controls:

   8.3.1. Unique user IDs so that activities can be attributed to the responsible individual.

   8.3.2. User lock-out controls after consecutive failed login attempts.

   8.3.3. Controls to terminate a User session after a period of inactivity.

   8.3.4. Password complexity requirements (requires letters and numbers).

   8.4. Security Procedures, Policies and Logging:

   8.4.1. User access log entries will be logged

   8.4.2. Logging will be kept for a minimum of 90 days.

   8.4.3. Logging will be kept in a secure area to prevent tampering.

   8.4.4. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

9. **Endpoint Protection:** Kernshell's Services have been designed to avoid the introduction of viruses to Customer's systems but may not scan for or prevent viruses or malware included in attachments, iterative data files or other data when provided by Customer to Kernshell. Kernshell utilizes endpoint protection on our servers and corporate end user devices.

10. **Information Security Program Changes.** Kernshell periodically updates and implements enhancements to the Information Security Program, and may add or modify security controls, procedures, policies, and features. These additions and modifications will not make the Information Security Program less protective than it was on the effective date of the Agreement in any material respect. We may revise these Security Standards at any time by posting a revised version at https://www.kernshell.com/terms-of-service/.