SECURITY STATEMENT

Date: April 9, 2024

This document outlines the security measures and protocols adopted by Governmentjobs.com Inc., also known as NEOGOV. Our commitment extends to various web services we offer, including but not limited to neogov.com, neoed.com, governmentJobs.com, schooljobs.com, powerdms.com, planitschedule.com, agency360.com, and cuehit.net. This excludes any services governed by separate terms and conditions. We are dedicated to safeguarding your data through a blend of physical, technical, and administrative measures, ensuring its integrity, security, and appropriate usage.

Physical Security
Our technical infrastructure and information systems boast SOC 1 and SOC 2 accreditations, emphasizing our commitment to stringent security standards. Data center security features round-the-clock surveillance, biometric entry systems, secure visitor logs, and robust entry requirements, ensuring an unparalleled level of physical security.

Compliance Achievements
We pride ourselves on meeting and exceeding industry standards, with certifications across various compliance frameworks including SOC2 Type II, NIST 800.53 Moderate, CJIS, HIPAA security rule, and PCI-DSS self-certification, demonstrating our unwavering commitment to data protection and privacy. NEOGOV is currently in the process of achieving FedRAMP, StateRAMP, and TxRAMP accreditations.

Access Control
Our technology resources are accessible exclusively through secured means such as MFA and VPN, backed by robust password policies that enforce the principles of complexity and security. Access is strictly need-to-know, with immediate revocation following employment termination.

Security Policies
We regularly review, update, and enforce our information security policies to adapt to emerging threats and ensure compliance in the markets we serve.

NEOGOV Personnel
NEOGOV ensures the integrity and security of its operations and customer data through comprehensive employee screening and ongoing education measures. Prior to employment, all NEOGOV employees undergo background checks to verify their suitability for their roles. Once onboard, they are required to participate in annual training sessions focused on security, privacy, phishing prevention, and role-specific responsibilities to bolster their understanding and capabilities in safeguarding sensitive information. Additionally, employees are subjected to phishing simulations to test and reinforce their vigilance against cyber threats. To further secure customer data, NEOGOV employs the principle of least privilege, strictly limiting employee access to information necessary for their job functions.

Dedicated Information Security Team
Our rigorous hiring process includes background checks in compliance with applicable laws. We emphasize the importance of information security through policy distribution and mandatory

non-disclosure agreements, ensuring that only authorized personnel access sensitive information.

Our dedicated Information Security Team is at the forefront of our security efforts, focusing on compliance, education, and incident response, ensuring a proactive stance against potential security threats.

Advanced Monitoring
Our system is under constant surveillance, with an on-call team available 24/7/365 to respond to alerts and deviations. This ensures that our security posture remains robust against all threats, including IDS/IPS, application-aware firewalls, WAFs, next-generation endpoint protection, file integrity, data loss prevention, and file scanning. All logs are centrally managed into an SIEM for the NEOGOV Information Security Team to correlate events across the environment.

Thorough Security Scanning
Security Scanning NEOGOV performs many different types of scans including Static and Dynamic code scanning, and weekly authenticated scans against the infrastructure and SaaS applications. In addition, NEOGOV maintains ongoing private and public bug bounty programs. Annually NEOGOV performs a third-party penetration test that includes a full network, application, and code vulnerability assessment.

Vulnerability and Patch Management
NEOGOV's patch management and remediation strategy is a cornerstone of our cybersecurity efforts. By adhering to the latest NIST guidelines, we ensure that our systems and data are protected against the latest vulnerabilities and threats, thereby upholding our commitment to security and trust.

Encryption and Data Protection
All data, whether in transit or at rest, is encrypted using industry-standard FIPS-compliant encryption methods. We enforce strict HTTPS and SFTP protocols to protect customer data, ensuring it remains secure and private.

Incident Management and Breach Notification
Our incident response policies are designed to address security breaches swiftly and efficiently, with mandatory customer notification and public communication protocols in place, adhering to legal and contractual obligations.

Business Continuity and Disaster Recovery
At NEOGOV, we prioritize providing our customers with exceptional uptime. To achieve this, we have developed a resilient infrastructure designed to eliminate any single points of failure through built-in redundancies. We rigorously adhere to our backup and retention policies, ensuring all NEOGOV data is securely backed up and replicated off-site. Our backup processes include continuous encryption and integrity testing, guaranteeing the reliability and safety of our data. In preparation for any unforeseen events, we have established a secondary data center and maintain several cloud availability zones in a state of readiness, allowing us to swiftly respond and restore services in the case of a disaster declaration.

Third-Party Management
NEOGOV maintains contractual data security and privacy obligations with our partners that send or receive personal information. The external security of NEOGOV's partners is monitored continuously and all partners are re-evaluated on an annual basis.

Defense in Depth
In addition to the aforementioned measures, we adopt a Defense in Depth strategy, layering multiple security controls across the organization to protect against a wide range of threats. This approach ensures that even if one layer is compromised, others are in place to maintain overall security.

Zero Trust Framework
We also implement a Zero Trust framework, which assumes that threats can originate from anywhere, thereby verifying every access request as if it originates from an untrusted network. This means not just relying on traditional security measures but ensuring that every request is authenticated, authorized, and encrypted, regardless of its origin. This framework complements our Defense in Depth strategy, providing a robust, multi-layered defense mechanism against potential security breaches.

Customer Security Responsibilities
The security of your data also depends on your vigilance. We recommend maintaining complex passwords and ensuring your systems are protected against targeted attacks such as phishing, as part of a comprehensive security strategy. Customers are also responsible for their user management and ensuring proper access controls when allowing access to their NEOGOV environments.

Our commitment to your data's security is unwavering, and we continuously evolve our strategies to combat emerging threats and vulnerabilities, ensuring the safety and integrity of your information at all times. If you would like more information please reach out to your NEOGOV Point of Contact for more information.