SECURITY STATEMENT

Date: Feb 14, 2023

This Security Statement applies to the web services offered by Governmentjobs.com, Inc. DBA NEOGOV, including the websites neogov.com, neoed.com, governmentJobs.com, schooljobs.com, powerdms.com, planitschedule.com, agency360.com, or cuehit.net, the subdomains and subdirectories of each, but excluding services that explicitly state they are subject to different terms and conditions. Where we have control of your data, we take our responsibility to implement security controls seriously. We implement physical, technical, and administrative safeguards to prevent unauthorized access, maintain accuracy, integrity, security, and facilitate correct use of personal information. The following is a brief overview of controls we have in place to protect your data.

Physical Security
Our information systems and technical infrastructure are SOC 1 and SOC 2 accredited. Physical controls at the data centers include 24x7 monitoring, biometric access and mantraps, cameras, visitor logs, entry requirements, and dedicated cages.

Compliance
NEOGOV have achieved the following certifications under various compliance frameworks. NEOGOV is SOC2 Type II 5 trust principles certified, NIST 800.53 Moderate certified, FedRAMP Ready, StateRAMP Fast Track Ready, CJIS certified, HIPAA security rule certified PCI-DSS self-certified.

Access Control
Access to our technology resources is only permitted through secure connectivity (e.g., MFA VPN). There are password policies in place to ensure complexity, length, and lifetime requirements are met. We grant access on a need to know basis and revoke access after employee termination.

Security Policies
We maintain and regularly review and update our information security policies. Employees must acknowledge policies and undergo annual job specific security and privacy training.

Personnel
NEOGOV conduct background screening at the time of hire (to the extent permitted or facilitated by applicable laws and countries) and rescreening for key job roles . We also distribute our relevant information security policies to all personnel and require non-disclosure agreements. Only authorized employees with a reasonable need related to their job duties have access to personal information. Employees who violate our policies are subject to disciplinary action, legal action and termination.

Security Personnel
NEOGOV has a dedicated Information Security Team responsible for security, compliance, education, and incident response.

Continuous Monitoring
NEOGOV has continous monitoring across the information system. In addition NEOGOV has a 24x7x365 on-call rotation with alerting on deviations from our baselines. This includes but not limited to real-time alerts based on availability, performance, IDS/IPS, Next-Generation Endpoint Protection, and SIEM findings. NEOGOV also has near-real time alerting based on external security posture of our products.

Security Scanning
NEOGOV performs weekly internal and external automated scans against the infrastructure and SaaS applications. In addition NEOGOV maintains an ongoing private and public bug bounty programs. Annually NEOGOV performs a third-party penetration test that includes full network, application and code vulnerability assessment.

Vulnerability Management
NEOGOV maintains an internal Plan of Action & Milestones (POAM) dashboard to track vulnerabilities, patching activities, and to ensure remediation is performed within specified timeframes. Severity and remediation timeframes follow recommended CISA and NIST 800-53 guidelines.

Encryption and Data Security
NEOGOV encrypts all data in transit and at rest using FIPS compliant encryption. Only TLS 1.2 ciphers are supported for HTTPS and SFTP access. Customer data is stored in the Data zone which is segmented from our DMZ zone. HTTPS traffic is terminated on the perimeter firewall, inspected and re-encrypted.

Information Security Incident Management
NEOGOV maintains security incident response policies and procedures covering the initial response, investigation, customer notification (no less than required by applicable law or contract), public communication, and remediation. These policies are reviewed annually.

Breach Notification
Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. NEOGOV's breach notification procedures are consistent with our obligations under applicable country, state and/or federal laws and regulations, as well as any industry rules and contractual commitments.

Business Continuity and Disaster Recovery
All NEOGOV data is backed up and replicated remotely according to the backup and retention policy. Backups are encrypted and tested continuously to ensure integrity. NEOGOV maintains a secondary datacenter and multiple cloud availability regions in the event of a diseater.

Third Parties
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.

Customer Responsibilities
Keeping your data secure also requires that you maintain the security of your accounts by using sufficiently complex passwords. You should also ensure that you have sufficient security on your own systems and data, and be vigilant of targetted credential attacks (i.e. phishing).