SECURITY STATEMENT

Date: November 17, 2021

This Security Statement applies to the web Services offered by Governmentjobs.com, Inc., including the websites “NEOGOV”, “NEOED”, “GovernmentJobs.com”, or “SchoolJobs.com”, 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 the security 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
Governmentjobs.com is SOC2 Type 2 certified, PCI-DSS self-certified, HIPAA Security Rule certified and NIST 800.53 Moderate certified. NEOGOV is also in the process of obtaining FedRAMP certification.

Access Control
Access to our technology resources is only permitted through secure connectivity (e.g., VPN). Our production password policy requires complexity, expiration, and lockout. 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 additional job specific security and/or privacy law training for key job functions.

Personnel
We conduct background screening at the time of hire (to the extent permitted or facilitated by applicable laws and countries) and rescreening. We also distribute our relevant information security policies to all personnel and require personnel to sign 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, up to and including termination.

Security Personnel
We have an Information Security Team responsible for security compliance, education, and incident response.

Vulnerability Management and Penetration Tests

We conduct periodic scans and remediation of security vulnerabilities on servers, network equipment, and applications. All networks, including test and production environments, are regularly scanned. Critical patches are applied to servers on a priority basis and as appropriate for all other patches. We also conduct regular internal and external penetration tests and remediate according to severity for any results found.

Encryption

We encrypt data in transit and at rest.

Information Security Incident Management

We maintain security incident response policies and procedures covering the initial response, investigation, customer notification (no less than as required by applicable law or contractually required), public communication, and remediation. These policies are reviewed regularly.

Breach Notification

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. Our breach notification procedures are consistent with our obligations under applicable country level, state and federal laws and regulations, as well as any industry rules or contractual commitments. We may seek to notify you by email.

Information Security Aspects of Business Continuity Management

Our databases are backed up on a rotating basis of full and incremental backups and verified regularly. Backups are encrypted and tested regularly to ensure availability.

Third Parties

We maintain contractual data security and privacy obligations with our partners that send or receive personal information.

Your Responsibilities

Keeping your data secure also requires that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems.