Information Security Overview

RESEARCH NOW SSI recognizes the importance of data privacy and data security and has established an Information Security program to manage RESEARCH NOW SSI's data security requirements and constantly monitor developing trends and threats. The program is led by qualified information security professionals who closely collaborate with RESEARCH NOW SSI's General Counsel to ensure that any contractual or regulatory data protection requirements are integrated into the information security program. The Information Security team leverages all the necessary departments and staff at RESEARCH NOW SSI to address security issues as they arise. A high-level overview of the technical, physical, and administrative safeguards that RESEARCH NOW SSI has implemented to protect customer data are described below.

Information Security Policies

RESEARCH NOW SSI has global information security policies, approved by management, and communicated to all employees and/or contractors that address the information security areas that are critical to RESEARCH NOW SSI. These policies include, for example:

- Information Security Policy
- Acceptable Use Policy
- Confidential Information Policy
- Global Privacy and Data Protection Policy
- Account Security (Passwords, Automatic Logoff, and Session Lock)
- Network Security
- Physical Security
- Technical Vulnerability Management

Information Security, Awareness, and Training

RESEARCH NOW SSI employees receive Information Security Training upon hire and the requirement to adhere to organizational policies is addressed and communicated via the employee handbook. As a general practice, contractors and 3rd party users must read and agree to abide by RESEARCH NOW SSI Information Security policies prior to gaining access to RESEARCH NOW SSI information systems. RESEARCH NOW SSI also provides training related to PII, PHI, and HIPAA.

With regards to customer data, RESEARCH NOW SSI employees receive training on how to handle information assets, including:

- Secure methods of data transmission and storage
- Secure practices for the handling of paper and electronic assets
- Secure practices for communicating oral information
- Assets that cannot be shared

Background Checks

In the United States, RESEARCH NOW SSI undertakes a background check on each prospective new hire as permitted by law to ensure compliance with applicable client agreements as well as to ensure a safe workplace for its employees. These background checks include a seven (7) year history of each individual. RESEARCH NOW SSI does not hire individuals with felony convictions and/or misdemeanor convictions for crimes involving fraud/dishonesty.

Datacenter Security

RESEARCH NOW SSI systems are located in third party full service co-location facilities which provide state of the art security that meet a number of compliance and/or third party certification standards including HIPAA, GLBA, SOC2 and/or SSAE 16. These facilities provide redundancy with multiple backup generators, uninterruptable power supplies and air conditioning units. Physical security controls include perimeter fencing, surveillance, on-site security guards, key card access, biometric systems, and mantraps to control and restrict access to data centers. Security cameras are placed throughout the data center facilities to record physical activity and are actively monitored 24/7/365.

Office Security

Physical security requirements for RESEARCH NOW SSI offices are communicated to the organization via employee training and company policy. While offices have varying levels of security, the objective for all offices is to prevent unauthorized access to Research Now SSI information systems and any data that is housed at the facility. Physical safeguards include: badge access, keys, fencing, gates, receptionist/security personnel, security patrols, visitor logs, biometrics, pin/key-based locks. Some offices have cameras.

Network Security

A network security policy has been published and communicated that outlines RESEARCH NOW SSI's requirements for network security. The following network security controls are implemented:

- External networks (Internet, extranets, external partners) are segregated from internal networks with firewalls.
- Internet facing servers and services are located in the DMZ network with firewalls in between.
- Firewalls are configured to deny all inbound connections by default and only allow based on application/system needs.
- Firewall rules are regularly reviewed.
- Network based Intrusion Detection and Prevention systems are deployed at the network perimeter.
- Internal network traffic is monitored for malicious activity with passive vulnerability scanners.
- Firewall Logs are sent to a log aggregation/correlation tool to detect indicators of compromise or other malicious network activity.
- Traffic is encrypted using HTTPS.

- Remote access to the RESEARCH NOW SSI network is limited by hardware firewalls and available to select employees through VPN access. Security features include Multi-factor authentication and encryption utilizing HTTPS.

Threat Management

RESEARCH NOW SSI has an IT Risk Assessment Program which includes:

- Monthly external and internal vulnerability scans.
- Annual independent network security assessments and a penetration tests.
- Standard practices for assessing all new servers for vulnerabilities and remediating findings before going into production.

Security Monitoring

RESEARCH NOW SSI has a security monitoring strategy with specific use cases to monitor for real-time cyber events, for example:

- Intrusion Detections
- Ransomware Detections
- Virus Detections
- Critical group or infrastructure changes
- Rogue AP detection
- Detections for Indicators of Compromise
- Detections for anomalous activity

Encryption

The use of encryption to protect information in transit and at rest is required by the RESEARCH NOW SSI Information Security policy. RESEARCH NOW SSI employees are required to work with IT Operations and Security to ensure that the method of data transmission used will utilize an acceptable encryption algorithm. When transmitting data with clients, RESEARCH NOW SSI recommends the use of its internally hosted secure transport system which utilizes SFTP and HTTPS for file transmission.

Data Destruction

When data is scheduled to leave organizational control (e.g. the disposal of assets) RESEARCH NOW SSI engages third-parties for the disposal of equipment and works with vendors that comply with the requirements of NIST Special Publication 800-88 and provide certificates of destruction. Any specific requirements for the secure disposal of data is determined on a project by project basis as set forth by client.

Additional Controls include:

- Routine encrypted backups
- Disaster Recovery for core systems

- Audit log management
- Change Management
- Controls against Malware (e.g. Anti-Virus, Web Filtering)
- Access Control
- User registration, modification and de-registration procedures
- Password policies
- Management of privileged access rights
- User registration, modification and de-registration
- Review of user access rights
- Software Development Lifecycle
- Independent Review of Information Security

Additional details about RESEARCH NOW SSI's Information Security Program can be provided once a Non-Disclosure Agreement (NDA) has been executed by both parties. If you would like RESEARCH NOW SSI to complete a more detailed vendor risk assessment questionnaire, please provide the document and the instructions to your RESEARCH NOW SSI business partner who can submit it to the RESEARCH NOW SSI Information Security team for review.