Client Confidentiality

At Directions, our marketing research role routinely puts us in contact with highly confidential information such as new or modified products, product concepts, marketing plans, as well as personally identifiable information (PII), and industry regulated data. We consider all client materials confidential information and they are kept in the strictest of confidence. As such, Directions operates under a comprehensive Information Security Policy highlighted throughout this document. Our staff is trained early and often on the importance of not sharing any information with staff who do not have a need to know. All client confidential and regulated data is kept in logically separated locations on our network, and access to client locations is restricted on a need to know basis.

Training is conducted on broader emerging threats through a continual security awareness program. Our staff is screened with a national criminal background check including a 7 year history and HHS-OIG & GSA name search. We also use a timed password protected screensaver on all end user systems and individual private offices with doors (no cubicles) for all staff. Further, we utilize locked shred bins located throughout the building. Shred bins are emptied and shredded onsite biweekly.

We also encrypt data on our mobile laptop fleet through whole disk encryption, regulated data at rest and in transit, and our data backup tape rotation.

Information Security Policy, Auditing, & 3rd Party Review of Controls

Directions' Privacy Officer, Director of Information Technology, and extensive information security policies ensure consistent application of security procedures across the enterprise. Our security policies are based on a hybrid of the CISSP, ISO 17799, and Bindview/Meta Security Groups' models with additions from sans.org. Information security policies are reviewed and acknowledged by staff annually. Extensive information security logging, monitoring, and auditing demonstrate our commitment to consistent and thorough operational security. Our security framework has been reviewed by Plante & Moran. Plante & Moran is the nation's 13th largest CPA advisory firm with over 2000 professionals and 22 offices spread around the globe.

In March of 2016, Directions successfully completed its annual SOC 2 Type II audit performed by Plante & Moran. A SOC 2, Service Organization Control Report (www.aicpa.org/soc), is issued under the AT Section 101 attest standard. It focuses on a business's non-financial reporting controls as they relate to security and confidentiality. The Type II variety tests the effectiveness of controls as executed over a six month evaluation period. During the same six month period, Directions completed a HIPAA/HITECH and GLBA review, also by Plante & Moran. HIPAA/HITECH are regulations associated with the healthcare industry. GLBA (Gramm-Leach-Bliley Act) is a regulation associated with the financial industry.

Directions also executes an internal audit program to monitor encryption procedures. Monthly, a subset of network storage containing regulated Personally Identifiable Information (PII) is selected. The subset is reviewed to identify compliance with the encryption policy. Encryption policy violations are reported to the Director of IT and can be escalated to the Privacy Officer.

Directions captures event logs on all servers and security infrastructure. With the exception of CCTV (90 days), logs are retained for 24 months. Our Solar Winds Log Event Manager server scans and notifies administrators on selected events. Additionally key logs are reviewed on a scheduled interval by a member of our IT staff. The intervals are specified throughout our policy set with security/boundary device logs receiving the highest scrutiny, followed by public facing servers, followed by critical infrastructure, and lastly support infrastructure. Additionally we have a series of policy enforced checks on our authentication repository (MS Active Directory) which include reviews of network accounts (creation, termination, & privileges) by the Privacy Officer.

As indicated in our Escalation policy, we also have a policy requirement to safeguard logs in the event of threat detection. Lastly, we utilize a message based log for events covering change management and approvals.

High Availability: Risk Assessment, Redundancy & Diverse Routing

Through an annual risk assessment, Directions systematically identifies opportunities for strengthened security and business continuity. Systems are classified into recovery tiers and disaster tested against expected outcomes. Annually our DR/BC plans are reviewed, tested, and approved by senior management.

These plans include critical services being hosted on platforms designed in redundant/clustered formations, ensuring always-online operation. Tier 1 systems that store and process client data, in addition to email, are mirrored to a second Network Operation Center (NOC). The second NOC is a vendor managed DR facility in a geographically dispersed location. Our SOC2/SSAE16 Type II audited partner, provides a fully managed facility freeing our IT staff to focus on the strategic recovery of our operations rather than focus on the day to day operation of the infrastructure. For protection against more isolated equipment failure, we utilize nightly data backups to a mix of disk and tape. Encrypted backup tapes are taken offsite weekly.

High availability is at the heart of Directions' Information Technology philosophy. Our data centers utilize multiple fiber carriers with ample bandwidth for Internet connectivity, dedicated cooling, and servers with redundant storage, power, fans, and communication interfaces. The facilities use battery backup and/or power generation equipment for continuous operation. Environmental controls (cooling, power, humidity, moisture, and fire) are monitored for immediate response. Our primary core network utilizes multiple backbone switches, routers, and firewalls with BGP routing of Internet fiber carriers to ensure failover and high capacity throughput.

Directions utilizes operating systems from Microsoft Windows & Red Hat and database products Microsoft SQL Server and MySQL; ensuring we have both the greatest features and support communities available. For analytical tools, an array of products from SPSS, SAS, Microsoft, and The R Foundation are available. Additional SAAS and cloud based solutions are employed for functionality such as encrypted laptop backup. All such solutions have been evaluated for their security risk.

Physical Security

Directions utilizes a number of methods to physically secure its primary facility. The building is configured with two tier perimeter access, first by unique (to each employee) numeric PIN at the building's entrances, followed by a badge access control to each floor of occupancy. Badge access is authorized by HR, with access activity audited quarterly. Badge access is terminated immediately for exiting staff.

External entrances and internal doors are configured with door prop alarms ensuring doors cannot remain open beyond 90 seconds. Further our staff is trained to prevent "tailgaters" from accessing the building and to question all unidentified visitors. We also utilize CCTV at our building and data center entrances. Lastly, data center entrances are monitored for a forced door event. Alarm escalation lists and procedures are reviewed quarterly. The forced door event escalation list includes IT professionals, senior management, facilities staff, and local authorities.

Visitors/vendors are required to register at the front desk. All visitors sign in and provide their name, company name, reason for visit, time of arrival and time of departure. Visitors are required to provide a government-issued photo ID (with the exception of routine visitors personally recognized by receptionist). Further, visitors are escorted at all times.

Logical Access and Electronic Security

To manage logical access, HR authorizes account creation and removal. Account removal is performed through a comprehensive exit checklist ensuring all physical, electronic, and third party account access is terminated. In addition, the Privacy Officer reviews privileged accounts & groups and performs quarterly account reconciliation reviews. We involve business relationship owners for client access control at the time access is requested and quarterly through a user access review. Similarly SFTP, Microsoft SharePoint and other portal access is reviewed on a quarterly basis. Prior to employee access, an employee background check and end user policy & security training are completed.

Our infrastructure is built on award winning Cisco switching, routing, security, and VOIP gear. Public facing security related configuration changes, such as firewall rules, require privacy officer approval. Such configuration changes generate change management alerts. We utilize a fully managed SecureWorks Intrusion Detection System to inspect

network traffic. In addition to system hardening, our network is scanned for vulnerabilities annually by a third party and internally on a quarterly basis. Our custom public facing applications undergo a full application penetration test.

Across the enterprise we centrally manage our anti-malware and patch management software with anti- tamper, reporting and administrator notifications enabled. With daily reviews of both systems we ensure our first line of defense is up-to-date. We also scan software on all devices regularly with follow up action taken to remove any unauthorized software installations.

For remote access, we utilize a mix of single and two factor VPN authentications based on user access level. When remote desktop is used, functions like clipboard and print local are disabled.

User accounts are centralized in Microsoft Active Directory with VPN, firewalls, routers, & switches using LDAP & Radius authentication. Further our email and UNIX infrastructure utilize single-sign on ensuring a singular authentication repository for password complexity, expiration, history, lock-out monitoring, and access reviews. In addition to system policies enforcing strong password complexity, an ethical password cracking procedure is run semi-annually.

Equipment Reuse & Destruction

As governed by our “Equipment End of Life” policy, all media & equipment capable of storing data are securely wiped/destroyed before disposal. All end user equipment is also wiped before it can be reassigned for new use.

Data Loss Prevention

We have an extensive policy set requiring data encryption of regulated data while at rest or in transit. We also use whole disk encryption on all laptop hard drives. We accomplish this with a combination of:

- An Information Receipt and Management Policy requiring the classification and handling of incoming data
- A Mobile Media Data Policy defining appropriate use of data on mobile devices
- An Encryption policy and procedure set
- Internal audits
- Industry standard encryption software

Further, our "need to know" data access procedures restrict the number of users with access to client data. Regulated client data, such as protected health information (PHI) and financial industry personally identifiable information (PII), have even tighter access groups with data loss controls prohibiting the use of USB & optical storage and unapproved file transfer services. We also conduct an ongoing awareness training and communication program as new risks emerge.

Vendor Management

Directions has a vendor security management program. We have a dedicated resource in charge of vendor compliance. This role includes classifying vendors based on data access and distributing key documents such as Vendor Services Agreements (VSA), HIPAA Business Associate Agreements, Confidentiality Agreements, and Security Assessments.