IMT Confidentiality, Privacy & Security Practice Standards Statement

Protecting the confidentiality, privacy, and security of client data is paramount in IMT. To ensure strong internal governance and full compliance to all laws, regulations, contracts, and client requirements, IMT has in place the following policies and controls:

A formal information classification scheme for all data.

An information handling policy identifying information custodians, processes required to access data, and regulations for the collection, storage, disclosure, and destruction of data.

A Corporate Security and Compliance Officer Systems accountable for ensuring audit, disclosure, and breach policies are in place and ensuring compliance to external legislation such as the Health Insurance Portability and Accountability Act (HIPAA).

Policies for compliance that are renewed annually including an employee code of conduct and confidentiality agreement.

Annual employee training on SOC2 controls, HIPPA compliance, ethics, and harassment.

SOC2 audits for compliance to the SOC2 trust principles of security, confidentiality, and privacy.

Bi-Annual formal reviews of the Corporate Risk Plan and BCP/DR Plan.

Minimum security standards for all employees and devices in IMT.

Cybersecurity insurance.

An internal support team responsible for managing data security, data availability, data access, and all audit and logging of data movement in IMT.

The following security principles are enforced within IMT:

Sensitive data (information classification IMT Restricted) is encrypted, stored behind firewalls, and protected from unintended disclosure with intrusion detection tools.

Network traffic may only be monitored for the express purpose of protecting the data assets of IMT and its clients, ensuring appropriate legal use and performance of the network, and meeting obligations to preserve and provide electronic information in connection with legal proceedings, investigations, and to address threats to IMT or individuals in a timely manner.

IMT Support must capture and retain network traffic as permitted and must capture and retain small amounts of network traffic related to specific vulnerabilities to identify security events or confirm a security incident, collect aggregate statistics about network use, and share de-identified or aggregate statistics within IMT.

IMT Support team's determination that access to an application or website should be allowed or disallowed must be based upon cybersecurity risk, not the content of the application or website.

IMT must implement fixes and remediation steps as soon as able based the severity and immediate need of resolution to an incident.