



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, incident handling 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, HIPAA 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 Emergency/Risk Plan and Business Continuity Plan/Disaster Recovery Plan.
- Minimum security standards and computing device requirements 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.
- Data Disposal and destruction policies are enforced for client systems and employee devices.
- Network Security and Storage Management policies are enforced for security, availability, data integrity, confidentiality and compliance
- 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.

YOUR ACCESS TO AND CONTROL OVER INFORMATION

You can do the following at any time by contacting us via compliance@imt.ca:

- See what data we have about you, if any.
- Change/correct any data we have about you.
- Have us delete any personal database information we have about you.
- Express any concern you have about our use of your data.

SECURITY

We take precautions to protect your information. Only employees who need the information to perform a specific job (for example, billing or customer service) are granted access to personally identifiable information. The computers/servers in which we store personally identifiable information are kept in a secure environment.

UPDATES

Our Privacy Statement may change from time to time and all updates will be posted to this document and at <https://www.imt.ca/our-story/privacy-policy/>

If you feel that we are not abiding by this privacy statement, you should contact IMT Company Security Officer, Meagan Caruk immediately via telephone at 204-989-4630 or via email at meagan@imt.ca or compliance@imt.ca.