



Privacy Policy

Summary of MTM Privacy Policy

MTM Technologies, Inc. (the "Company" or "MTM"), **Privacy Policy** is a statement that discloses some or all of the ways MTM gathers, uses, discloses and manages MTM customer or client's data. While performing business, MTM collects information that is important for servicing its clients and customers. This policy declares how privacy information is collected, stored, and personal information released. It informs MTM clients of what specific information is collected, how it is kept confidential, and shared with MTM partners for business purposes.

Specifically, MTM information privacy, or data privacy (or data protection), is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.

Privacy concerns exist wherever personally identifiable information or other sensitive information is collected and stored – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.

As the laws and regulations related to data protection are constantly changing, it is important MTM to keep abreast of any changes in the law and continually reassess compliance with data privacy and security regulations and inform its client and partners of any changes.

Data that MTM collects

In order to utilize our Services we need to collect certain data about our customers. Some of the data we collect is customer/client and personal data in that it will be capable of identifying the client or the individual. For instance your name and address.

When you use our service we will collect, store and use the following kinds of customer/client and personal data:

- Data provided when you register for an event;
- Data provided when you use any services we provide;
- Data about your computer such as your IP address and use of our website (eg. frequency & length of visits, pages visited);
- Account information which includes customer name, address, telephone number, e-mail address, service-related details such as payment data, security codes, service history and other similar information;
- Network performance & usage information that tells us how the customer uses our network, our products and our services, and how well our products and services are performing;

Basic ways of collecting data

- a) We collect information when a customer makes a purchase;
- b) We collect information on how you use our products and services;
- c) We collect information when we sign contracts with new accounts, vendors, partners, etc.
- d) We collect information during electronic and mailing correspondences with our clients, customers, etc.



4 High Ridge Park – Suite 102, Stamford, CT 06905

866-383-2867

mtm.com

Use of collected data

MTM will use customer/client and personal data collected in the following ways:

- To provide and administer MTM services to our clients, customers, partners, etc.
- To administer our customer loyalty program;
- To operate the website from a technical and practical perspective;
- For internal record keeping;
- For the purposes of customer care (for instance, responding to complaints);
- To provide services and improve client's customer experience;
- Send financial statements/invoices for purchased services and products;
- Respond to client's questions and inquiries;
- Address network integrity and security issues;
- Do research and analysis to maintain, protect, develop and improve our products and services; and,
- Inform clients about service updates, offers, and promotions, if applicable.

Data Protection

Principles governing the protection of personal data are:

1. Notice—data subjects should be given notice when their data is being collected;
2. Purpose—data should only be used for the purpose stated and not for any other purposes;
3. Consent—data should not be disclosed without the data subject's consent; information collected by an individual cannot be disclosed to other organizations or individuals unless authorized by law or by consent of the individual
4. Security—collected data should be kept secure from any potential abuses; records kept on a client or individual should be accurate and up-to-date
5. Disclosure—data subjects should be informed as to who is collecting their data;
6. Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; there should be mechanisms for individuals to review data about them, to ensure accuracy; this may include periodic reporting;
7. Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles;
8. Data should be deleted when it is no longer needed for the stated purpose;
9. Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited; and,
10. Some data is too sensitive to be collected, unless there are extreme circumstances (e.g., sexual orientation, religion).

Also, MTM uses several security systems and procedures to safeguard the information, ensuring the data is accessed only by authorized individuals for legitimate business needs. MTM will not transmit or sell the compiled information to third parties without obtaining a written or electronic agreement that defines the rights and responsibilities with respect to the data. Further, MTM will review our clients' use of data to ensure sensitive data is being handled in accordance with required protections, and that this information is not used for deceptive, misleading, or suspicious purposes.

Our Privacy Principles

We depend on your cooperation and trust, and we promise to protect the confidentiality of your information. The MTM Technologies, Inc.'s Privacy Principles remind us of this promise and help ensure the protection of your information throughout all of our activities.



4 High Ridge Park – Suite 102, Stamford, CT 06905

866-383-2867

mtm.com

The Privacy Principles are our guidelines. They help us as we design surveys to consider respondents' rights and concerns. Every principle embodies a promise to you, the respondent.

- **Necessity:** Do we need to ask this question? Do we need to collect this information? Every time we prepare to ask a question, we determine whether the information is truly necessary. All of the information we collect is used for providing services to our customer and partners.
 - We promise to collect only information necessary for customer service purposes.
 - We promise we will use the information only to service our clients timely and communicate with them for customer service purposes.
- **Openness:** Do you know why we are collecting your information?
 - We collect information only for customer service purposes, and it is never used to identify individuals.
- **Respectful Treatment of Respondents:** Are our efforts reasonable and did we treat you with respect?
 - We promise to minimize the effort and time it takes for you to participate in the data collection by efficient designs.
 - We promise to use only legal, ethical and professionally accepted practices in collecting data.
 - We promise to ensure any collection of sensitive information from children and other sensitive populations does not violate federal protections for research participants and is done only when it benefits the public good.
- **Confidentiality:** How do we protect your information?

In addition to removing personally identifiable information, such as names, telephone numbers, and addresses, from our data files, we use various approaches to protect your personal information; including computer technologies, statistical methodologies, and security procedures. Our security measures ensure that only a restricted number of authorized people have access to private information and that access is only granted to conduct our work and for no other purposes.

We promise that every person with access to your information has signed a Confidential Information, Solicitation and Proprietary Property Agreement during hiring process. According to MTM Associate Guide, MTM employees and contractors must "must maintain the confidentiality of information entrusted to them by the Company, its customers, partners, or business associates and any other confidential information about or related to the Company its customers, partners, or business associates that comes to them, from whatever source, in their capacity as a director, officer or employee of the Company, except when disclosure is authorized or legally mandated. For purposes of this Code, "confidential information" includes all non-public information relating to the Company, its customers, partners, or business associates". Non-compliance is conveyed to employee's supervision for corrective action. MTM conducts pre-employment checks on all potential employees. In addition, MTM also conducts criminal background checks, Social Security Number verification, driving history (if applicable) and education verification (if needed).

- We promise that we will use every technology, statistical methodology, and physical security procedure at our disposal to protect your information.
- All MTM employees are made aware of MTM's policy via the MTM Associate Guide and required to sign a document acknowledging their awareness

MTM Online Privacy Policy for Children

We want you to know that we do not knowingly collect personally identifying information from anyone under the age of 13 unless we first obtain permission from the child's parent or legal guardian.



4 High Ridge Park – Suite 102, Stamford, CT 06905

866-383-2867

mtm.com

MTM Privacy Commitments

- We do not sell your personal information to anyone for any purposes.
- We keep your personal information in our business records while you are a customer, or until it is no longer needed for business, tax, or legal purposes.
- We will keep your information safe using encryption or other appropriate security controls.

Customer California Privacy Rights

California Civil Code Section 1798.83 entitles California customers to request information concerning whether a business has disclosed Personal Information to a third parties for their direct marketing purposes. As stated in this Privacy Policy, we will not sell your Personal Information to other companies and we will not share it with other companies for them to use for their own marketing purposes without your consent.

'Cookies' and internet tags

A cookie is a file that is stored on your computer which allows our website to recognize that your computer has accessed our website previously. We use cookies to collect and process anonymous information about your visit to our website such as, which pages you visited; how long you spent on those pages; how often you visit it. We will use this information to improve the contents of our site or to collate statistics about it, or to otherwise improve and customize our services to you. You can set your computer to refuse to accept cookies and to delete current cookies held on your computer but this will likely have a negative effect on your use of our website (for instance because the website will no longer recognize your computer). You can get more information about cookies from www.allaboutcookies.org.

Security

Transactions over the internet are not in themselves secure so we cannot guarantee the security of the customer/client and personal data that you provide to us. We will however take reasonable technical and organizational measures to prevent the loss or corruption of your data in accordance with US data protection legislation.

Google Analytics

The Google Analytics features we have implemented are based on Display Advertising (e.g., Remarketing, Google Display Network Impression Reporting, the DoubleClick Campaign Manager Integration, or Google Analytics Demographics and Interest Reporting).

Using the Google Ads Settings, users can opt-out of Google Analytics for Display Advertising and customize Google Display Network ads. We use Remarketing with Google Analytics to advertise online.

Visiting Other Websites

Our website contains links to other agencies, private organizations, etc. These websites are not within our control and may not follow the same privacy, security, or accessibility policies. Once you link to another site, you are subject to the policies of that site.

Data Governance

Data Delivery Process

MTM supports in-transit data encryption to secure the communications between our systems and those of our clients. In-transit data encryption is performed via SSL/STTPS (Secure Socket Layer/Hypertext Transfer Protocol Security, supported by Entrust for certificate authority), SFTP (Secure File Transfer Program), public/private keys, and SSH (Secure Shell).



4 High Ridge Park – Suite 102, Stamford, CT 06905

866-383-2867

mtm.com

Information Exchange Policies and Procedures

Whenever a computer network connection is established between an MTM computer and another computer at a location outside an official MTM office, and whenever this connection transmits or is likely to transmit "confidential" information, the link must be encrypted. Such encryption must be accomplished only with systems approved by the IT Department. These systems include virtual private networks that incorporate not only encryption but also approved user authentication mechanisms.

Exchange Agreements

MTM executes NDA (Non-Disclosure Agreement) with clients as contracts are negotiated and signed. Additionally, client contracts outline the requirements of data exchange and may include the following:

- Identification of who is responsible for controlling and notifying transmission, dispatch and receipt on either side of the agreement;
- Notification procedures to ensure that the other side knows that sensitive information has been dispatched or received, and associated (primarily technical) controls to ensure traceability and nonrepudiation;
- Minimum technical standards for packaging and transmission;
- Courier identification procedures;
- Responsibilities and liabilities if data are lost or there are information security incidents;
- The agreed labeling system, to ensure that the appropriate protection required is immediately obvious and provided; the preferred system should (practically) be the same as that used by the receiving organization internally, as this will ensure that there is consistency of understanding;
- Where relevant, responsibilities for information and software ownership, and for data protection, software copyright and ownership and similar issues;
- Where relevant, technical standards for recording and reading information and software;
- Any special controls (such as cryptographic) that may be necessary for particularly sensitive information.

Security Overview

The security of our clients' data is the most of the utmost importance to MTM. We have a team of dedicated technologists and security personnel solely focused on ensuring that our systems, facilities, and applications are reviewed for risk, both natural and manmade.

This team has implemented, and continuously updates, a comprehensive enterprise-wide information safety and security program/training. The program/training functionally combines practical, cost effective technical solutions with sound management practices to provide a level of security that:

- Protects sensitive, critical, and proprietary information from unauthorized access, disclosure, or modification;
- Protects information systems and supporting computer resources from accidental or deliberate loss, damage, or destruction;
- Ensures the integrity, confidentiality, and availability of information assets and computing resources;
- Recognizes and adheres to all federal and state regulations concerning the dissemination of copyrights, patents, and data;
- Protects the privacy of individual users while assuring appropriate use of MTM assets.

User Access Management

MTM requires information system users to be assigned a unique identification (user-id) for access information resources. To ensure access control, users authenticate themselves to their user-ids by inputting a unique password. Users are authorized for only those access privileges necessary to perform their job assignments.



4 High Ridge Park – Suite 102, Stamford, CT 06905

866-383-2867

mtm.com

The IT team is also responsible for disabling and removing network access once a user has terminated their relationship with MTM. Network access is disabled upon employee termination.

Only authorized MTM staff is granted access to MTM and clients' information resources. Authorized staff granted access are restricted to specific defined, documented and approved applications, databases, supporting data files, and operating system platforms. This includes access to administrator, root or super user accounts on production data systems, applications and platforms. Our system proactively monitors every log on of a privileged account. This information is then verified to ensure the correct people have administrative or privilege access.

Users are authorized initially with a secured temporary password, which they are forced to change immediately on first logon. Users are issued temporary passwords if they forget their own passwords; this is only done after the user has been positively identified. Temporary passwords are unique to an individual and not guessable, and are delivered securely to users; (they are sent in clear text, but not in the same message as the user-id information). Passwords are never stored in or on computer systems in clear view. System hardening standards require that default vendor passwords on every single item of computing hardware be changed on installation.

Passwords are required of all users assessing tools and databases containing data. Account passwords must adhere to the following MTM standards:

- Unique user account/user-id
- Passwords must be at least eight characters long
- Passwords must be "strong", that is, composed of at least three of the following four categories: upper and lowercase letter, special character and/or numerical character.
- Users are required to change the initial password upon first login.
- Passwords must be changed at least every 90 days.
- The system is configured for an 8-password history that cannot be reused.
- Accounts are locked out after three invalid login attempts.

Network Security

Our external network is protected via firewall and a secure zone, which is also separated from the internal production zone via a firewall. Systems in both zones require unique user-ids and passwords for access. Both zones are monitored 24x7 by MTM IT systems. The IT team is responsible for managing and maintaining the operation of the firewalls.

Our systems include virus prevention software at the firewall, server, email and desktop levels. MTM uses antivirus software programs to help safeguard our network and to protect desktops and file server systems.

Information Backup

Backups are performed on a daily, weekly, and monthly basis. The IT team controls the duration of backups and how much to be retained based on regulatory requirements. The backup software confirms successful data backup after each backup prior to finalizing the backup process.

Disaster recovery

Continuity of corporate business and client hosting is critical at MTM. As such, MTM focuses on our ability to avoid disasters as much as we focus on our ability to recover from disaster. This includes utilizing top tier redundant hardware in datacenters as well as designing failover into our daily operations. MTM utilizes a number of strategies to avoid MTM or client system downtime. Some ways are: a) Data centers that are monitored 24/7, b) redundant hosting infrastructure, c) maintenance and refreshing our hardware proactively with up-to-date technology to eliminate disruptions due to aging equipment and out-of-date components - all hardware is reviewed annually, d) highly available system design – all core



4 High Ridge Park – Suite 102, Stamford, CT 06905

866-383-2867

mtm.com

pieces of MTM infrastructure are clustered and hosted solutions can also be designed and deployed with clustering to provide desired levels of system availability and reduce single points of failure within the architecture; e) process control – MTM ensures that all changes to production systems are reviewed for quality and are approved for customer release. We also review metrics to ensure our systems are designed and operating at the appropriate levels to meet the performance and capacity demands of our clients.

Privacy & Data Protection Policy

This privacy policy sets out how we collect and use personal and other data that you provide to us when you use our website & MTM services. We respect your privacy and so we collect and process all data in accordance with US data protection legislation currently in force.

This policy may be changed from time to time by updates to this page. Please review this policy on a regular basis to ensure your overall awareness. If you have any questions on our policy please e-mail us at hr@mtm.com.



4 High Ridge Park – Suite 102, Stamford, CT 06905

866-383-2867

mtm.com