TEEMA Privacy & Security Data Policies

Created:	Policy Revision Date:	Intended for the use of:
Nov. 2019	February. 2025	TEEMA Consultants

PART ONE. PRIVACY.

OVERVIEW/PURPOSE

The privacy policy contains the policies and procedures for TEEMA Solutions Group Inc. and TEEMA Inc. Under the direction of the Privacy and ITO Officers, these policies have been designed to comply with The Freedom of Information and Protection of Privacy Act. These policies have been designed to apply with the operations of the company as a Service Provider, in order to remain compliant with Health Organizations in Canada.

The purpose of this policy is to educate TEEMA personnel on how to act in the utmost professional way surrounding privacy and personal information, in order to protect the use and disclosure of Personal Information. TEEMA aims to educate personnel and help to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information. This document seeks to display how TEEMA will make reasonable arrangements against risks of privacy breaches, unauthorized disclosures and collection of PI.

SCOPE

This policy applies to all TEEMA employees, members and representatives (“personnel”) working directly for TEEMA and/or providing services to a Client, regardless of how the PI is stored, formatted or recorded. All personnel have a responsibility to read and adhere to this privacy policy, as well as any amendments or modifications that may be introduced from time to time. This includes when off duty and extends beyond completion of employment.

DEFINED TERMS

- Company means TEEMA Solutions Group Inc. and TEEMA Inc.
- HO means Healthcare Organization.
- ITO means Information Technology Officer.
- PI means personal information. Examples include:
    - An individual’s name, address, telephone number, personal healthcare number;
    - An individual’s race, national or ethnic origin, colour or religious beliefs or associations;
    - An individual’s age, sex, sexual orientation, marital or family status;

- An individual's fingerprints, blood type or inheritable characteristics;
- Information about the individual's health care history, including physical or mental disability;
- Information about an individual's education, financial, criminal or employment history; and
- Opinions about an Individual
- Personnel means any employee of TEEMA, HQ, or a contractor/subcontractor means providing services for TEEMA

- TEEMA HQ – Employees working in TEEMA's Head Quarters in Vancouver, BC.
- TEEMA means TEEMA Solutions Group Inc. and TEEMA Inc.

POINTS OF CONTACT

The Company is committed to ensuring the privacy of Personal Information. The Company will designate and maintain an internal Privacy Officer position. The Privacy Officer will be responsible for the development and implementation of the Company's policies and procedures regarding privacy, personal information and FIPPA laws. The Privacy Officer will be trained on all policies and procedures necessary to fulfil his or her responsibilities in ensuring the privacy of Personal Information. Questions or concerns about collection, access, use, processing, or disclosure of PI can be directed to the Privacy Officer.

Designated Privacy Officer for TEEMA:

Rachel Bettney
Title: HR Compliance Officer
Email: **compliance@teemagroup.com**
Direct Phone Number: 778-357-0758
Toll Free: **Toll-Free:** 833- MY–TEEMA (833-698-3362) Ext: 7799

The Company is committed to ensuring security of all data. The company will also designate an Information Technology Officer (ITO). The ITO will be responsible for the development and implementation of the Company's policies and procedures regarding security and data. The ITO will be trained on all policies and procedures necessary to fulfil his or her responsibilities in ensuring the security of Personal Information.

Designated ITO for TEEMA:
Lane Babuder
Title: Technical Operations Officer
Email: it@teemagroup.com
Toll Free number: **Toll-Free:** 833- MY-TEEMA (833-698-3362) Ext: 7788

ETHICS

TEEMA has and expects a high standard of ethics and expects that all TEEMA personnel and contractors follow the following standards of behaviour at all times in the hope that these ethics minimise any breaches of privacy, alongside the other policies and procedures defined in this document.

Honesty
TEEMA personnel are expected to conduct their business honestly, fairly and transparently.

Confidentiality
TEEMA personnel shall maintain the highest degree of integrity in all their dealings with clients and or other personnel, both in terms of normal business continentality, and protect all personal and (or) corporate information received in the course of providing business services.

Duty of care
The actions and advice of TEEMA personnel shall always conform to relevant federal, provincial and (or) territorial laws, regulations and (or) standards. Their actions should respect the human rights of people in the organizations with whom TEEMA interact in business.

Contracts
TEEMA personnel will always strive to meet the contractual requirements of the company's clients and fully disclose in a prompt and transparent manner any activities that require modifying those contractual requirements.

Professional Conduct
TEEMA personnel shall conduct all their business activities professionally and with integrity. They strive to be objective in their judgement and any recommendations so that issues are never influenced by anything other than the best interests of TEEMA's clients.

PRIVACY REPRESENTATIVES

The Privacy Officer and ITO will be trained on the requirements of FIPPA and the Company's policies and procedures regarding the privacy of PI, including but not limited to:

(a) the secure transmission and storage of Personal Information in any form;

(b) the rules on accessing Personal Information;

(c) the secure management of Personal Information;

(d) individual rights regarding Protected Health Information;

(e) contracts with all personnel and subcontractors and rules surrounding Personal Information

(f) the proper use of the notice of privacy practices;

(g) the retention of records and appropriate documentation regarding privacy;

(h) the complaint procedure;

(i) internal training requirements;

(j) notification requirements in the event of a Breach of Unsecured PI

Training will be conducted for the Privacy Officer and ITO as soon as reasonably practicable. In the event that a different person than initially trained assumes the role of Officer and ITO training for such person will be conducted as soon as possible after such person assumes the role of Privacy Officer or ITO.

ACCOUNTABILITIES

Governance: Accountability for TEEMA compliance with this Policy rests with the Compliance Team, although other Staff is responsible for day-to-day collection and processing of PI. TEEMA personnel have a responsibility to oversee compliance with this policy within their area(s) of responsibility. All members of staff have responsibility to ensure that appropriate steps are taken to protect PI at all times. They must ensure that their practices in collecting, accessing, using, processing, or disclosing PI comply with this Policy as well as with FIPPA and provincial requirements and their professional codes of practice. In addition, Staff are expected to report to the TEEMA Compliance Team (Privacy Officer and ITO) any concerns with or recommended improvements to information privacy and security procedures, and any information to help resolve problems.

Acknowledgement of Confidentiality. TEEMA will make all Staff aware of the importance of maintaining the confidentiality of PI. As a condition of employment or affiliation, all new Staff must read this Privacy Policy and sign an approved Confidentiality Acknowledgement. In addition, PI obtained in the course of one's employment or other affiliation with TEEMA must be held in confidence even after the affiliation comes to an end.

ACCESS

Access to Protected Health Information must be reasonably limited only a job related 'need to know'.

RELEASE OF INFORMATION

No personnel may release any PI about an individual to any Party unless expressly authorized by the Relevant Laws.

CHANGES

The Company will change the Policies and Procedures as necessary and appropriate to comply with changes in the law. The Company may also change its Policies and Procedures at any time, for any reason. The Company may not implement any changes to the Policies and Procedures until such changes are documented and, if necessary, are reflected in a revised Notice of Privacy Practices.

PROTECTING PRIVACY

TEEMA Personnel working for a client:

Personnel should position their computer screens so that the screen is not visible to visitors or other persons in the work area, if possible.

Such personnel shall log off any software systems containing such PI at the end of each day.

In addition, such personnel shall not leave their computer unattended without logging off such software systems, minimizing the screen or engaging a locked screen saver, and must log off such software system minimizing the screen or engaging a locked screen saver, when visitors or persons without appropriate access to such information are in close proximity to allow their view of such information on the computer.

Personnel must follow any password change and computer use policies.

Personnel must use a screen lock to prevent access to their workstations when not logged off the system.

Personnel must lower voices and move to a secure place to discuss PI with other personnel for a job 'need to know' basis only.

SUBCONTRACTORS

Subcontractors will be expected to comply with all the necessary precautions outlined above.

OBTAINING AUTHORIZATION

For all uses of PI, other than those required by law the company will obtain an authorization that is signed by the individual. The purpose of obtaining an authorization is to provide the individual with an opportunity to determine how his or her PI may be used or disclosed, and to inform the individual of his or her rights.

COMPLAINTS PROCEDURE

TEEMA encourages and has a procedure dedicated to receiving complaints from individuals regarding compliance with the requirement of FIPPA and the use of PI. The company will take on and look into complaints about any aspect of their practices regarding PI. For example, individuals would be able to file a complaint when they believe PI relating to them has been used or disclosed improperly; that an employee has improperly handled the information; that they have wrongfully been denied access to or opportunity to amend the information; that the Company's notices do not accurately reflect their information practices; or that the covered entity has not provided the appropriate notices required due to breach.

The Privacy Officer and ITO should be contacted in order to file a complaint concerning the Company's policies and procedures, or their compliance with such policies and procedures.

The Privacy Officer and ITO will immediately report the complaint to management (Operations Manager and the Vice President); and promptly investigate any complaint, take appropriate remedial action if a violation of the Company's policies and procedures has occurred and apply appropriate sanctions. The Privacy Officer and ITO will also ensure that all applicable notices are provided in accordance with the Company's policies and procedures.

PASSWORDS

The Company seeks to ensure the integrity, confidentiality and availability of electronic PI.

The Company, therefore, recommends the use of passwords to ensure such protection. Passwords Support Our Use and Disclosure Policies and Procedures. To ensure that only authorized users gain access to our information systems in order to appropriately use and/or disclose PI, authorized users, as a means of authentication must supply Individual user passwords. These passwords must conform to certain rules contained in this document. Passwords must never be shared and should never be written down.

TIPS:

- ✓ Keep system-level passwords secret and refrain from sharing password information with anyone other than authorized Company personnel.
- ✓ Create passwords at Company that are unique and different from passwords used for
- ✓ personal accounts.
- ✓ Create unique formats for passwords (refrain from using simple ones such as your DOB. Use a mixture of lower case and upper-case letters, numbers and symbols).
- ✓ Change your password every 3 months or when prompted.

FAILURE TO COMPLY

The Company has established and will apply appropriate sanctions against members of their workforce, as well as other personnel, who fail to comply with their policies and procedures.

This policy is designed to give guidance and ensure compliance with applicable laws and regulations related to sanctions for violating the Company's policies and procedures. The type of sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors.

Sanctions may include but not limited to:

(a) Additional training on the policies and procedures

(b) Written warning

(c) Final warning

(d) transfer/demotion

(e) Termination of employment

(f) Termination of contract in case of contractor

CONTRACTORS

TEEMA contractors providing a service on behalf of TEEMA to HO's may receive, create, transmit and maintain PI. For the purpose of this policy, contractors are classed as TEEMA personnel.

All contractors are subject to the same privacy policies and procedures as TEEMA HQ personnel.

TEEMA aims to enforce and monitor these procedures by entering into an agreement with these contractors and providing a training manual and guidance on policies and procedures.

TEEMA commits to updating these policies when the law requires a change, or annually. Whichever comes first. Contractors will be trained annually or when policies have been updated.

If a contractor refuses to sign and acknowledge the agreement and policies, and the contractor may access to PI in order to perform services on behalf of TEEMA, TEEMA shall not contract with the contractor.

A copy of this document will be maintained by TEEMA.

BREACHES OF PRIVACY

All privacy violations shall be reported in a timely manner to the Privacy Officer and ITO. The importance of reporting all actual or suspected privacy breaches cannot be overstated. When incidents or violations are reported, they can be corrected.

In the event of a privacy breach involving PI it must be reported to a supervisor and the Privacy Officer and ITO.

In accordance with FIPPA standards, once notified, TEEMA intends to report and mitigate the breach by the following steps:

1. Contain the Breach
2. Risk Analysis
3. Contact the Authorities
4. Notification to relevant parties and authorities
5. Rectify outstanding issue(s) that led to breach and take any other necessary steps to prevent future breaches. All TEEMA HQ staff would be notified in order to remain on 'high alert'.
6. TEEMA will keep track of all incidents using a 'Security Breach Notice Log'. This includes all of the information above and resolution steps for next time. TEEMA reviews this quarterly, should we have any incidents. This is in order to track any possible patterns and put in place extra steps to try to prevent a breach happening again.

The Privacy Officer and ITO shall train all workforce personnel and contractors with access to PI on these policies and procedures and to report any possible Breach of Unsecured PI to the Privacy Officer and ITO immediately.

USEFUL LINKS

The following is a non-exclusive list of relevant laws, regulations, etc. that TEEMA is legally or contractually bound to abide by when handling PD and/or PHI. This list is merely for reference and may change from time to time.

EU-U.S. Privacy Shield Frameworks: The EU-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to

comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. Onward Data Transfer Agreement – The Framework requires in Principle 3 b that in order to transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request. Link: https://www.privacyshield.gov/welcome

More information about **Health Insurance Portability and Accountability Act (HIPAA); (US Healthcare);** Can be found at the link below. National standard in the United States to protect individual medical records and other personal health information and applies to health plans, healthcare clearing houses, and those health care providers that conduct certain healthcare transactions electronically. TEEMA is contractually bound to be HIPAA Compliant as a Business Associate. LINK: https://www.hhs.gov/hipaa/for-professionals/index.html

More information about **Personal Information Protection and Electronic Documents Act (PIPEDA);** can be found at the link below. Federal privacy law in Canada for private-sector organizations that sets out the ground rules for how businesses must handle personal information in the course of commercial activity. LINK: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personalinformation-protection-and-electronic-documents-act-pipeda/

More information about **The Freedom of Information and Protection of Privacy Act (FIPPA);** (Canadian) can be found at the link below. An information rights law that gives an individual a legal right of access to records held by relevant Canadian public bodies, subject to specific and limited exceptions. LINK: http://www.bclaws.ca/civix/document/id/consol26/consol26/96165_00;

PART TWO: DATA AND SECURITY.

PURPOSE

1. Purpose

This data security policy is built to enforce adherence to any applicable laws under any jurisdiction in which TEEMA operates its businesses.

2. Scope

2.1 This data security policy applies to all customer data, personal data, or other company data as defined as sensitive or private under any applicable laws within jurisdictions.

2.2 Information that is classified as Public is not subject to this policy, other data can be excluded when used for specific business needs as adhered to applicable laws within jurisdictions.

3. Policy

3.1. Principles

TEEMA will provide the necessary facilitations for appropriate training and information to these policies as are applicable to employees, members, and consultants.

3.2. General

a. Each user is assigned a unique address so that any actions taken within TEEMA's used systems are logged and the user can be held accountable if actions must be taken.

b. The use of shared identities is permitted only where suitable, such as training.

c. All users will read and adhere to this policy.

d. Records of user access may be used to provide evidence for security incident investigations

e. Access shall be granted based on the principle of least privilege; this means that users will only be granted access to the level in which they are needed to perform the tasks they are given.

3.3. Access Control Authorization

a. Access to company IT resources and services will be given through the provision of a unique user account and a password. Accounts are provided by the onboarding department.

b. Password requirements for length, complexity, and expiration are enforced by the IT Department.

3.4. Network Access

a. Employees of TEEMA with access to physical offices TEEMA operates will be granted network access in accordance to the needs as defined by their role.

b. Employees of TEEMA will be granted VPN access to specific network functionality as are applicable to their role.

3.5. User Responsibilities

a. All users must lock their screens whenever they leave their device to reduce the risk of unauthorized access.

b. All users must keep their workplace clear of any sensitive or confidential information when they leave.

c. All users must keep their passwords confidential and shall not share them.

3.6. Application, Data, and Information Access

a. All TEEMA employees, members, and contractors will be granted access to the data and applications required for their job roles.

b. All TEEMA employees, members, and staff shall access sensitive data and systems only if there is a business need to do so and have approval from higher management.

c. Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

3.7. Access to Confidential, Restricted information

a. Access to data classified as 'Confidential' or 'Restricted' shall be limited to only authorized persons whose job responsibilities require it.

b. The responsibility to implement access restrictions lies with the IT Department

3.8. Additional Training As Contracts Require

4. Technical Guidelines

Access control methods to be used shall include:

- Auditing of attempts to log on to any account in which TEEMA utilizes a login system or service.
- Role based access model
- Server Access Rights
- Firewall Permissions
- Web authentication rights

- Encryption is required and enforced on all data in transit and at rest for any and all devices when used with TEEMA

5. Reporting Requirements

All TEEMA employees, members, and consultants are required to immediately report any data incidents they become aware of.

The IT department will conduct regular audits of applicable devices and accounts with access to any data. At minimum these audits will occur once per year.

A TEEMA IT Staff will make continual audits of TEEMA security, and policy enforcement on all TEEMA employees and consultants where applicable at minimum on a quarterly basis with compliance reports being issued.

All audit reports will be submitted to an operational member of staff.

6. Enforcement

Any user found in violation of this policy is subject to disciplinary action, up to and including termination of employment.

Any third-party partner or contractor found in violation may face the same actions and may have any access granted immediately revoked.

1. Security, Threat, and Risk Assessment Policy

TEEMA will conduct regular security threat and risk assessment audits as outlined within the ISO27000 standard series and as revised. At minimum these audits will happen at least once per year.

8. Data Storage Location Compliance

a. TEEMA will adhere, to the best of its abilities, to regional limitations on storage of client data where applicable.

b. In the event that certain data cannot be stored within the jurisdiction of a TEEMA client's request, that client will be made aware of this limitation. These limitations may include.

   i. The use of certain types of cloud storage, or cloud service providers

   ii. TEEMA employees that may reside outside of the jurisdiction

9. Access to Client Data

Access to TEEMA client data will only be provided to those who may need this data in order to perform their role as adherent to the principle of least privilege.

Any disclosure of client data to third parties must be previously approved by the client except in the event of legal warrant or investigation.

10. Data Security Audit Report Requests from Third Parties

Audit reports may be requested by clients, vendors, and law enforcement as is reasonable, in accordance with contracts, and within applicable laws.

11. Security Roles

TEEMA will assign roles to employees within legal jurisdiction where applicable.

Example:

- TEEMA has a presence in the United States, and Canada, as such there are employees within each jurisdiction, TEEMA will assign Security Officer Roles for each of these jurisdictions.
    - Current Canada Security Officer:
        - Steve Reimer
    - Current United States Security Officer:
        - Lane Babuder
    - Current International Security Officer:
        - Rachel Bettney

(Page left intentionally blank)

CONFIDENTIALITY ACKNOWLEDGEMENT

- ✓ In consideration of my relationship with TEEMA, I acknowledge and agree as follows:
- ✓ I have read, understand and will adhere to this Privacy and Security Data Policies as amended from time to time, concerning the collection, use, processing, and disclosure of PI, as defined herein and in the Relevant Laws, obtained in the course of my relationship with or provision of services to TEEMA; I understand that all PI is confidential and may not be communicated to anyone in any manner, except as authorized by TEEMA, or Relevant Laws;
- ✓ I will adhere to the laws governed by PIPEDA, FIPPA, HIPAA (depending upon the country I am working in).
- ✓ I understand and acknowledge that all information regarding TEEMA, including corporate, financial and administrative records, is confidential and may not be communicated or released to anyone in any manner except as authorized by TEEMA, or applicable policies;
- ✓ I understand I must protect all PI in my possession from theft or loss. This includes but is not limited to, keeping the information with me at all times, storing it in a locked and secured area when unattended, and encrypting and password protecting it when stored on electronic mobile devices (e.g. USB drives, laptops, etc.);
- ✓ I will not copy, alter, interfere with, destroy or remove any confidential information or records except as authorized by TEEMA in accordance with established policies;
- ✓ I understand that access to PI is only for the purpose of and limited to what is required to perform my role. I will not access my record or those of family, friends or others, unless I am directly involved in providing care or other services to the individual the information is about;
- ✓ I will immediately report to the Compliance Team (Privacy Officer and ITO) the potential or actual unauthorized disclosure or loss of any PI;
- ✓ I understand that compliance with this Policy is a condition of my relationship, employment or service contract with TEEMA and that failure to comply may result in immediate termination of my employment or services, in addition to legal action by TEEMA and/or others.
- ✓ By accepting these terms, I am confirming that I acknowledge, understand and agree to the above.

Signature

Date

TEEMA Privacy Disclosure

Created:	Policy Revision Date:	Intended for the use of:
Nov. 2019	February. 2025	TEEMA Consultants

YOUR PRIVACY IS IMPORTANT TO US

Protecting the privacy and confidentiality of personal information has always been a fundamental principle in our business relationships. We want you to know that TEEMA Solutions Group and TEEMA Inc. adhere to privacy legislation that governs what information may be collected, how it is used and how it is protected. This Privacy Statement explains our privacy policies and information handling practices.

PROTECTING YOUR PRIVACY MEANS

- We keep your personal information and the business you do with us in strict confidence
- We do not sell your personal information
- You have control over how we obtain, use, and give out personal information about you
- You have reasonable access to the personal information we have about you
- We respect your privacy when we market our services

WHY WE COLLECT PERSONAL INFORMATION

We collect information in order to represent you for employment opportunities with our clients, to carry out surveys, to administer our web site, and to provide information about our services. We understand that some of this information is personal. We collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances. The information we will collect from you includes, but is not limited to:

- Your personal profile via your resume and information supplied by you
- Your employment preferences, such as work location, salary, and other personal factors important to you

You can visit our web site without sharing any personal information. While visiting our site, you may choose to provide information in the form of a resume.

WHAT WE DO WITH PERSONAL INFORMATION

When you provide personal information to us in the form of a resume or references, the information will be stored in our secure database. We may use your personal information to:

- Match your profile against our client's requirements
- Contact you regarding profile matches
- Contact and obtain information about you from references supplied by you

(upon your approval, see "Your Information is Obtained or Used Only with Your Consent")

- Provide your information to clients (upon your approval, see "Your Information is Obtained or Used Only with Your Consent")
- Carry out surveys
- Improve our site and, where applicable, the services we offer
- For other similar or related purposes that are reasonably necessary for the proper management of TEEMA Solutions Group Inc's. and TEEMA Ins'. business
- We may send you information about our company and promotional material from some of our partners from time to time. If you have concerns about receiving occasional communication from us, please contact support@teemagroup.com

TEEMA Solutions Group and TEEMA Inc. PLACEMENTS.

When you are placed with one of our clients, we will collect additional information in order to complete the placement process. In addition, we may survey you to ensure that we are offering our consultants the best possible opportunities and to provide our clients with constructive feedback. We will survey clients to verify and confirm the information we currently have in your file and to ensure our consultants are consistently meeting client expectations.

Please note that all active contract consultants will receive communication from TEEMA Solutions Group and TEEMA Inc. containing pertinent information related to current placements.

YOUR INFORMATION IS OBTAINED AND USED ONLY WITH YOUR CONSENT

We want to assure you that any personal information you provide to TEEMA Solutions Group and TEEMA Inc. will remain completely confidential until you request otherwise, unless required by law. We do not sell or provide candidate or client information to third parties. We will always obtain your authorization to contact references and we will always contact you via email or telephone before we submit your profile to a client.

YOUR CONSENT CAN BE EXPRESS OR IMPLIED

Express consent can be verbal or written. You imply consent when we reasonably conclude that you have given consent by some action you have taken, or when you decide not to take action. For example, by providing your contact information, profile or other personal information to a recruitment consultant or through our web site, you are granting your consent to allow TEEMA Solutions Group and TEEMA Inc. to use your profile information in the matching process, and to contact you regarding any such matches.

YOU CAN WITHDRAW YOUR CONSENT AFTER YOU'VE GIVEN IT

While we would like your consent to continue to collect and use your information as outlined above, we want you to know that you do have choices. In addition, you can request to have your information removed from our database, or opt out of receiving optional future mailings at any time by contacting support@teemagroup.com

WE PROTECT YOUR INFORMATION FROM ERROR, LOSS, AND UNAUTHORIZED ACCESS

Our employees who have access to your information are made aware of how to keep it confidential. Each employee is governed by policies regarding information handling. Only employees who require access to your information in the course of their duties will have access to your information.

We respect the confidential information that we receive from others and therefore will not release any personal information provided to us by third parties without their explicit authorization.

YOU CAN SEE AND VERIFY THE ACCURACY OF YOUR INFORMATION

You can update your personal information at any time by contacting support@teemagroup.com If you would like access to the personal information, we have on file for you, we will ask you to put your request in writing. You will be given reasonable access to your personal information to verify or correct information. Every effort will be made to respond to your inquiry within 30 days. There may be circumstances where TEEMA Solutions Group and TEEMA Inc. will not provide you with access or may require additional time to meet your request, in which case you will be informed.

LINKS TO OTHER SITES

Our site may contain links to other sites that we think you might be interested in. While we try to link only to sites that share our high standards and respect for privacy, we are not responsible for the content, security, or privacy practices employed by other sites.

COOKIES

Our site uses cookies to keep track of user sessions. Cookies improve functionality and, in some cases, provide visitors with a customized online experience.

CHANGES TO THIS PRIVACY STATEMENT

TEEMA Solutions Group and TEEMA Inc. reserves the right to modify or supplement our privacy statement at any time. If we make any changes, we will update this site to include such changes and post a notice on our home page for a period of 30 days, with a link to the updated privacy statement. If you return to this site after a period of more than 30 days, please check this privacy statement to confirm you are familiar with the most recent update. Your continued use of the site will constitute your consent to the changes, including use of personal information previously provided, as if they were the initial terms. However, we will seek your consent if we want to use your personal information for purposes other than those agreed to previously.