IMCORP™
Power Cable Reliability

IMCORP
Privacy Policy

Table of Contents

1.0 Introduction

This privacy policy is established to provide insight on what information or data Instrument Manufacturing Company (“IMCORP”) collects from its vendors, partners, and customers (whether an individual or a business entity, each an “Entity” or collectively “Entities”), the reasoning associated with that information collection, and the policies and guidelines IMCORP follows to ensure the security of such information or data.

For questions about this policy, please contact us at 860.783.8000 or via mail at:

IMCORP
135 Sheldon Road, Unit F
Manchester, CT 06042

IMCORP reserves the right to change or amend this privacy policy from time to time.

2.0 What IMCORP Collects

- **Customer account and information:** This includes information an Entity provides to create accounts or register for events, webinars, surveys, and may include, but not be limited to, first name, last name, a password, and a valid email address.
- **Physical Location Information:** IMCORP may collect an Entity’s physical location-based information for the purpose of providing and supporting services provided and for fraud prevention and security monitoring.
- **Physical Device Information:** When an Entity uses IMCORP services, IMCORP may automatically collect information on the type of device an Entity uses, operating system version, and device identifiers.

3.0 What IMCORP does with the information

IMCORP may access and use the information and data provided by, or collected from, an Entity as necessary (a) to provide and maintain the services; (b) to address and respond to service, security, and customer support issues.

Some specific, but non-exhaustive, examples of how IMCORP uses information provided by, or collected from, an Entity:

- Create and monitor user accounts
- Provide information on product updates, marketing communications, and service information
- Respond to inquiries and support technical requests
- Conduct research and analysis
- Analyze data, including through automated systems and machine learning to improve IMCORP services and/or end-user experience

4.0 Cookies

IMCORP will also continue improving our websites and products with the use of cookies, which help IMCORP understand how visitors use our websites and desktop tools. IMCORP owns this data but does not share this type of data with third parties.

Sample of Cookies Collected:

Cookie Type	***Purpose***	***Description***
Session Cookies	Website operation	Some cookies are essential for the operation of IMCORP websites. If a user chooses to disable these cookies, the user will not be able to access all the content and features.
Security Cookies	These cookies are used for general security purposes and user authentication.	We use security cookies to authenticate users, prevent fraudulent use of login credentials, and protect user data from access by unauthorized parties.

5.0 Information Sharing

IMCORP does not share Entity personal information with third parties except for certain logistical information such as work site addresses and locations which are necessary for executing our operations in conjunction with third party contractors.

6.0 Entity Security Responsibilities

IMCORP follows generally accepted standards to protect the information submitted to us, both during transmission and once it is received; however, no security measure is perfect. IMCORP recommends that the Entity safeguard any passwords created by the Entity or provided by IMCORP in order to access IMCORP services, as it is one of the easiest ways to manage the security of provided accounts. By using the IMCORP website, each Entity assumes the risk of unauthorized access of such Entity's information.

Entities are encouraged to expressly advise IMCORP of any confidential information or data to which IMCORP personnel have been granted access. Such data must be marked or otherwise designated "confidential". Refer to IMCORP's Data Classification Policy for additional guidance.

7.0 IMCORP Security Responsibilities

The following describes how IMCORP personnel handle vendor, customer, and partner information:

- Personnel are directed to access confidential information or data only to perform their job function.
  Personnel are directed to not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Personnel are directed to protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do their job or the action is approved by their supervisor.
- Personnel are directed to report any suspected misuse or unauthorized disclosure of confidential information immediately to their supervisor.
- If confidential information is shared with third parties, such as contractors or vendors, such contractors or vendors are required to execute a confidential information or non-disclosure agreement governing use of confidential information. Refer to the IMCORP's Vendor Risk Management Policy for additional guidance.

8.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.