Science.
Applied to Life.™

3M™ Connected Safety Data Privacy and Security

You and Your Data

Every day we navigate our way through our environment we are part of data that is collected and stored. Sometimes this data is directly tied to us as individuals, but in other cases, we are one part of a greater enterprise. The data can be used to discover important details about human behavior that can drive us towards a safer, more perceptive world. This is one of the primary elements behind 3M's decision to launch 3M Connected Safety—a platform to help you move your organization's worker health and safety program to a higher level, by incorporating the power of data.

At 3M Connected Safety, we want you to know that your data privacy and data security are respected. We want you to be confident in your choices when it comes to your safety-related data handling needs and 3M Connected Safety programs, while also knowing that you will get best-in-class service to support your worker protection program. The first consideration in any process involving sensitive personal and organizational data is trust, and 3M has made a commitment to be direct and honest about how your data is handled.

The following document has been created with you in mind to help you understand how 3M Connected Safety works to keep your data private, safe, and secure. In it we cover many aspects of our data privacy and security practices. It would not be possible or practical in this document to convey all the extensive steps we take to keep your data secure and private, but we offer this as a starting point for an ongoing conversation about the shared partnership we have to keep your valuable data safe.

3M Connected Safety Data Privacy and Security Values

3M Connected Safety employs the well-established data practices used throughout data-sensitive industries to keep your data safe and maintain its privacy. We like to summarize this as follows:

> **3M Connected Safety uses industry-standard data security practices that assume and respect our customers' rights to data privacy. The 3M Connected Safety platform uses state-of-the-art access control and credentialing, user logging, and encryption, and is localized on secure cloud servers that conform with the most demanding global security requirements. Our IT data governance policies, standards, and practices ensure that our customers remain in control of their data and that we serve their needs as the provider of worker protection connected solutions.**

What does this mean for you?

To be able to provide you with connected personal protective equipment for robust worker protection and effective asset management solutions, it is easy to understand that the 3M Connected Safety platform will need to have access to your operation's relevant data, but we want you to know that you always remain in control. All the data that we will collect and how we will use it are identified in our service agreements with you, with our role as a data processor and your role as the data controller fully described.

We will collect, aggregate, and analyze data generated within the Connected Safety platform to be able to improve our worker protection solutions that we can deliver to you, but it is not our business model to sell any data that can be identified with your workers or organization for advertising or other unrelated or undisclosed purposes, on our own or with any third party. To put it plainly, 3M cares about your autonomy when it comes to data, and we strive to be up-front and honest about how we use it to support your efforts to improve your organization's worker health and safety.

Cloud-based Software as a Service

3M's Connected Safety product platform is delivered to our customers with a Software as a Service (SaaS) model. This provides many advantages, including enabling an important data handling partnership with our secure cloud service provider so we can stay as up-to-date as possible with our security practices across the system. This also allows us flexibility, such as to designate geo-localized server locations as necessary for compliance to regulations. In addition to enabling us to deliver a high degree of security, SaaS allows us to maintain a high level of uptime to meet our customers' needs for reliable system access.

Technical Details

- The 3M Connected Safety cloud platform is built utilizing a distributed state-of-the-art architecture.
- The 3M Connected Safety system uses a platform as a service (PaaS) cloud structure through a leading cloud services provider.
- Cloud services enable us to scale across virtually any client size.
- Extensive security controls are in place to ensure data is segregated on a per-client basis.
- Data stored on secure cloud servers is only accessible by the service provider partner in response to a documented and logged 3M Connected Safety maintenance request or legal order, as defined in contractual agreements.
- Since the 3M Connected Safety system is deployed via the cloud as a web application, users are not required to install patches, updates, or urgent hot fixes. Instead, these are usually delivered as version updates.
- Users are notified whenever maintenance operations are being performed if service impacts are anticipated.
- Redundancy, load balancing and similar features are part of the service level agreement with our cloud services vendor and may be adjusted as necessary.

What does 3M do to keep your data safe?

3M has been handling customers' sensitive data privately and securely literally since before computers existed. Effective data privacy and security requires a multifaceted approach coupled with organization, discipline, and constant vigilance. When you join the 3M Connected Safety platform, you can be confident that 3M will continue to earn your trust by delivering data security and privacy through these and other actions.

Application Security

3M Connected Safety Applications must pass both black box and white box testing prior to deployment. Security and penetration testing are performed for all components of the 3M Connected Safety system, including the web application, data API's and mobile applications.

Only a strictly controlled set of vendor administrators can access your data. For customer support issues, only a strictly controlled set of administrators can access your 3M Connected Safety data.

3M Connected Safety uses secure, encrypted https channels for web and mobile transactions. Data at rest is protected via authentication, encryption, user security roles, token-based access control, and other methods.

The application system provides a System Admin role to persons defined by the customer.

A dedicated service monitors the 3M Connected Safety operation full-time.

All product environments are configured to auto-notify in case of issues.

The customer subscriber's security process can be leveraged administratively to provide additional application access security.

Physical Security

A high level of physical site security and site access control is in place both within the 3M organization that supports and administers the Connected Safety platform and our secure cloud services partner.

Disaster Recovery is performed via common industry practices including rolling backups and geographically segregated data centers.

Network Security

Strong passwords, encrypted channel communications, and layer security authorizations protect client data from unauthorized access.

General network security includes use of directory-based services in combination with network and IP filtering processes.

Network access to perform operations within the Connected Safety platform is subject to credentialing, permitted access rosters, and user access activity logging.

Our secure cloud services conform to virtually all global security certification requirements.

Connected Safety customer data uses hardware encryption at the device level, TLS 1.2 over HTTPS for data in transit, and AES 256-bit encryption for data in storage.

Data Support

Standards, policies, and procedures are maintained and updated to provide the structure of our Connected Safety IT data governance.

3M Connected Safety has procedures in place to respond quickly and effectively on a multinational corporate scale if necessary if a data incident occurs.

Technical support can be reached by calling a toll-free number.

Users can also request support via email at support-connectedsafety@3m.com.

In instances of service termination, customers may request removal of their identified data from the system, consistent with contractual terms.

Making Smart Data Choices for Your Worker Protection Solutions

For over one hundred years 3M has been earning the trust of its customers with the quality of its products and exceptional after-sale support. When you make the 3M Connected Safety platform part of your worker protection program, you are gaining access to not only the broadest, most capable portfolio of personal protective equipment, but also benefit from the full weight of 3M innovation applied to data-enabled worker protection solutions.

Personal Safety Division
3M Center, Building 235-2W-70
St. Paul, MN 55144-1000