Corsmed Security Policy

2026-03-10

The Corsmed platform is built to be easily accessible and user-friendly, a simple way to train, practice and research MRI. Openness and ease of use are valuable and important aspects of the Corsmed value proposition to our users.

Keeping your data secure is extremely important to us, and we spend a lot of effort and time to ensure all data sent to Corsmed is handled securely. With that said, you can still share URLs, ID or other information to make the usage non-secure, and we cannot take responsibility for security that is breached by the fundamental openness of the platform or sharing information you should not have.

Corsmed AB, Reg. No. 559093-1779, is hereinafter referred to as **“we”, “us”, “our”** or **“Corsmed”** and **”you”** shall be interpreted as the person or entity who has signed up for an Account to use our Services.

Any capitalized words used but not defined herein shall have the same meaning ascribed to them in the Terms & Conditions available at https://corsmed.com/legal (the <Terms=). The following capitalized words have the following definitions:

"Account" means the account you create or that we create for you to access the Services and Software, identifiable by email;

"User" means any person, such as a Customer, Free User or Team Member, who has signed up for an Account or in any other way use the Services;

"User Data" means all data (e.g., documents, text and pictures), including personal data, submitted by you electronically in the use of the Software, Services and Websites;

1. Human Resource Security

We have a process to ensure that all personnel with access to systems or information that can have access to information about our Users, as well as User Data have agreed to a non-disclosure undertaking as part of their employment contract with Corsmed. Our staff onboarding process includes verifying the identity of staff and the background and skill they state. Our rigorous staff termination process includes revoking access rights, seizing IT equipment, invalidating the company access card, as well as notification of continuous confidentiality obligations. Any staff with access to information about users shall be required to take appropriate security training on a regular basis as set out in the Security Revision Schedule below. When employment has ended, we revoke all access that the concerned employee had.

Roles, accountabilities and responsibilities

Chief Executive Officer

- Accountable for all aspects of Corsmed's information security and data processing.
- Determines the privileges and access rights to the resources within their areas.
- Responsible for the security of the IT infrastructure.
- Plans against security threats, vulnerabilities, and risks.
- Implements and maintains Security Policy documents.
- Ensures security training programs.
- Ensures IT infrastructure supports Security Policies.

- Responds to information security incidents.
- Helps in disaster recovery plans.

All Employees

- Must uphold and meet the requirements of Corsmed Security Policy.
- Report any actual, attempted and/or suspected security breaches.

In consideration of being entrusted rights to use Corsmed's systems, repositories and information all employees must acknowledge the following:

- That all confidential information must be kept confidential and that any disclosure of confidential information would cause harm to Corsmed.
- That employees will not, directly or indirectly, make use of information other than in the course of work duties;
- That employees will keep passwords, PIN codes, etc. entrusted to the employee, strictly confidential;
- That employees use, whenever possible, at least 2-factor authentication for systems with user data. We also require password-protected SSH keys.
- Firewall enabled on all workstations
- That employees will log off the computer or activate the screensaver configured with password immediately upon completion of each work session;
- That the employee understands that his/her rights to use Corsmed systems, repositories and information expire upon the termination of their work duty, or at any time upon the request by Corsmed. If the employee is not otherwise instructed, Corsmed requests that the employee shall immediately return all intellectual properties that the employee holds when his/her rights have expired.
- We only use well-recognized and highly secure 3rd party systems with proper security certifications and practices.
- Corsmed Password Control Policy defines the requirements for the proper and secure handling of passwords in the organization. All employees who handle assets and services related to Corsmed use password management via a certified password management system and strong passwords are required.

2. Operations security

Physical access to Corsmed's office premises is restricted to staff individually and on a need-to-have basis.

Physical access to where the Services are performed shall log physical access-related events, such as date, time, swipe/proximity card-id, door-id, access denied or access granted.

In addition, at Corsmed, we have a principle to protect your data called the principle of least privilege (PoLP), meaning that every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.

Losses, theft, damages, tampering or other incidents related to IT assets that compromise security must be reported as soon as possible to the Chief Executive Officer.

3. Business continuity and continuous improvements

We reserve the right to disconnect the Software for service and upgrades without giving prior notice to you, even though our intention is to give you notice before updates or maintenance of the Software. Please see the Terms for more information. We also reserve the right to implement new updates and versions of the Software, to the extent deemed suitable by us. We have a world-class engineering practice to ensure everything we do has a security perspective and a third-party vendor does penetration testing on a regular basis and reports threats in accordance with CVSS. High vulnerabilities are fixed within two weeks, medium within six weeks, low within eight weeks.

This list is an example of things we do to uphold information security with engineering practices:

- Clear code conventions enforced by static code analysis;
- Use of well-known frameworks to protect against common attack vectors (XSS, CSRF, SQL Injection);
- Incident response plans are maintained and followed to quickly act on incidents;
- Continuous check-up to keep libraries up-to-date;
- Continuous integration builds and testing;
- Continuous improvement process with the entire product team where security issues are a standing item;
- All code is peer-reviewed to find bugs and security holes early;
- Passwords are always kept in password safes or as a configuration.

4. Data Security

Processing

We are working with the best-in-class service providers for data storage. The service providers' physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate

Corsmed mainly utilizes the Amazon data centers defined as eu-west-1 (Ireland) and us-east- 1 (N. Virginia).

Amazon security is covered here:

- https://aws.amazon.com/security/

Security measures are taken to protect you and your data both for "Data at rest" and "Data in transit".

Data at rest

We use encryption of all Data "at-rest" and get powerful and automatic protection through our database provider. Read more here: + https://aws.amazon.com/security/
As described above and in the Privacy Policy, Corsmed stores Data on AWS (an Amazon service https://aws.amazon.com/compliance/) servers. We logically separate customer data in order to ensure integrity and confidentiality. Corsmed utilizes ISO 27001, SOC2 and FISMA-certified data centers managed by Amazon. Credit card information is stored with a PCI-compliant third-party vendor (Stripe). See Payment Details below for more information.

Data in transit

We use TLS (Transport Layer Security) on all connections, commonly referred to as SSL, which encrypts data between your browser and our server so no one can intercept it in transit. Privacy and protection of user data are of the highest importance to us, and we both have technical and operational support in place to ensure this.

Backups and Data Loss Prevention

Data is backed up continuously, and we have an automatic failover system if the main system fails. We receive powerful and automatic protection through our database provider.

User Password

We encrypt (hashed and salted) passwords to protect them from being harmful in the case of a breach. Corsmed can never see your password, and you can self-reset it by email. User session time-out is implemented, meaning that a logged-in user will be automatically logged out if they are not active on the platform.

Payment Details

We use PCI-compliant payment processor Stripe for encrypting and processing credit card payments. We never see or handle credit card information.

Security Incidents

We have in place and will maintain appropriate technical and organizational measures to protect personal data as well as other data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing (a "Security Incident").
We have an incident management process to detect and handle Security Incidents which shall be reported to the Chief Executive Officer (erik.jacobsson@corsmed.com) as soon as they are detected. This applies to Corsmed employees and all processors that handle personal data. All Security Incidents are documented and evaluated internally and an action plan for each individual incident is made, including mitigatory actions.

5. Security Revision Schedule

This section shows how often Corsmed conducts security revisions and conducts different types of tests. If significant changes occur Corsmed will initiate an otherwise planned activity to ensure continuing security.

Planned activity	**Frequency**
Security training for personnel	Yearly and at beginning of employment

Revoke system, hardware and document access	At end of employment
Ensures access levels for all systems and employees are correct	Yearly
Audit of Access management process and catalogue	Yearly
Firewall settings verification for workstations and Network	Yearly

Ensure all critical system libraries are up-to-date	Continuously
Unit and integration tests to ensure system functionality and security	Continuously

This Security Policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.

6. Contact

Corsmed AB is a Swedish limited liability company with registration number 559093-1779 and registered in Sweden.

You can always reach us at info@corsmed.com.

7. Changes to this Security Policy

This Security Policy is not part of the Terms, and we may change this Security Policy from time to time. Laws, regulations and industry standards evolve, which may make those changes necessary, or we may make changes to our business. We will post the changes to this page and encourage you to review our Security Policy to stay informed. If we make changes that materially alter your privacy rights, we will provide additional notice through the Services or via email if you have subscribed to notification in the link set out below. If you disagree with the changes to this Security Policy, you should deactivate your Account.