Corsmed Security Policy

2020-11-18

The Corsmed platform is built to be an easily accessible and 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, hereinafter referred to as **“we”, “us”, “our”** or **“Corsmed”**. **”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 uses the Services;

"User Data" means all data (e.g. documents, text, and pictures) including personal data, submitted by you electronically whilst using the Software, Services and/or 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 a performed background check and a thorough review of the skills that they have stated. 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.

We have implemented a rigorous staff termination process. Upon termination the employees access rights are revoked, IT equipment is seized, and we immediately invalidate the employees company access card. Moreover, we ensure to notify terminated employees of their continuous confidentiality obligations.

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.

- Continuously assesses security threats, vulnerabilities, and risks for preventative purposes.
- 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 the Corsmed Security Policy.
- Report any actual, attempted and/or suspected security breaches.

As all employees are entrusted rights to use Corsmed's systems, repositories, and information the following must be acknowledged:

- Any confidential information may not be disclosed, especially since confidential information may adversely affect and even harm Corsmed or its affiliates.
- Confidential information may not, directly or indirectly, be used other than in the course of each employee’s respective work duties;
- All entrusted authorization codes, e.g. passwords and/or PIN codes must be kept strictly confidential;
- Whenever possible, at least two-factor authentication for systems with user data must be used;
- Use of password protected SSH keys are mandatory;
- A firewall and full-fledged security software must be enabled on all workstation computers;
- Upon completing each work session (including shorter breaks) all computers must either be logged off or a password protected lock-screen must activated;
- The right to use any Corsmed systems, repositories and information expires upon termination of their work duty, or at any other time if requested by Corsmed;
- Unless instructed otherwise, Corsmed requests that the employee shall immediately return all intellectual properties that the employee holds when his/her rights have expired;
- Only well-recognized and highly secure 3rd party systems with proper security certifications and practices are to be used;
- Corsmed’s Password Control Policy defines the requirements for when passwords are properly and securely handled within the organization. All employees who handle assets and services related to Corsmed use password management via a certified password management system which is why strong passwords is a requirement.
- Use of VPN zones for connections to critical infrastructures

2. Operations security

Physical access to Corsmed's office premises is restricted to staff individually and on a need to 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. However, our intention is that such notices before updates and/or maintenance of the Software is performed. 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 where threats are reported in accordance with CVSS. High vulnerabilities are fixed within two weeks, medium vulnerabilities within six weeks, and low vulnerabilities within eight weeks.

The list provided below is used to exemplify things we do to uphold our information security in accordance with engineering practices:

- Clear code conventions enforced by static code analysis;
- Well-known frameworks to protect against common attack vectors (XSS, CSRF, SQL Injection) are used;
- Incident response plans are maintained and followed allowing us to act quickly in the event of an incident;
- Continuous check-up is performed in order for us to keep our libraries up-to-date;
- Continuous integration builds and testing is performed;
- Improvement processes are continuously implemented with the entire product team where assessment of security issues is a standing item;
- All code is peer-reviewed which enables discovery of eventual bugs and security holes early on;
- Passwords are always kept in password safes or as configuration;
- Architecture, design patterns, systems configuration and coding are all compliant to security best practices;
- Every connection of any system/node/module/process/end user’s workstation to another is encrypted (SSL);
- Penetration tests are running regularly to spot and assess potential breaches.

4. Data Security

Processing

We are working with top tier service providers for data storage. The service providers' physical infrastructure is hosted and managed within Amazon's secure data centres and utilize Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

Amazon's data centre 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 utilize the Amazon data centres defined as eu-west-1 (Ireland) and us-east-1 (N. Virginia).

Amazon’s security measures are 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 on all Data "at-rest" and get powerful 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 therefore separate customer data 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 SSL on all connections. Privacy and protection of user data are of 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 automatically be logged out if they are inactive whilst logged in 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 both personal and other data are in place and will be continuously be maintained. Our measures to protect such data have the purpose of hindering accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure, or access, as well as all other unlawful forms of processing (commonly referred to as 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 bring forward a 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 earlier if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness.

6. Contact

Corsmed AB is a Swedish limited liability company with company 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. If you disagree with the changes to this Security Policy, you should deactivate your Account or contact us with such a request.