Security Statement

We've provided an overview of the measures we take to secure your data.

Integrity and honesty are the key attributes of everything we do at Castor. We are committed to protecting our customers' data above all else.

Castor is secured according to the most recent standards in order to protect your data in the best possible way. Castor is certified for ISO 27001 (Standards for Information Security Assurance), the standard that describes how Information Security should be organized in a process-based manner in the context of the general business risks for the organization. Inspect our certificates or contact us if you'd like to learn more.

General application security principles

- Application code uses modern techniques to minimize the risk of SQL injection, cross site scripting (XSS) and other common attacks.
- We follow the OWASP top 10 to create awareness and inform ourselves about the most common vulnerabilities.
- Immutable audit logs provide a fine-grained overview of data access and modifications.
- All data is encrypted in transit and at rest.
- Yearly Penetration Tests ensure our application and infrastructure security is always up to date. Potential vulnerabilities can be reported via our Responsible Disclosure program.

Security of Castor EDC

- Users have individual accounts and strong passwords are required. Users are locked out of their account after 10 failed login attempts.
- Sessions automatically time out after 20 minutes of inactivity.
- Domain Administrators can enforce additional security policies, such as mandatory two-factor authentication or regular password rotation.

- Fine-grained, role-based access control is managed by the study administrator and authorization to study data is granted on a per person per institute basis. All access is denied by default, preventing unauthorized access.
- Study access can be limited based on IP-range in addition to requiring mandatory two-factor authentication.
- In addition to our default encryption of data at rest and in transit, an extra application-level encryption layer can be enabled for sensitive data. This uses encryption keys managed off-site by a trusted third-party key management system. Within the application, fine-grained encryption and decryption authorizations can then be granted per study and institute. Data is encrypted with libsodium's XSalsa and XChaCha streaming ciphers with Poly1305 MAC.

Security of Castor eConsent

- Users have individual accounts and strong passwords are required. Rate-limiting is used to prevent brute-forcing of passwords.
- Sessions automatically time out after 20 minutes of inactivity.
- Access to data is determined by the study and/or organization admin. This is done by assigning roles to users on an organization, study or site level.
- In addition to our default encryption of data at rest and in transit, an extra application-level encryption layer is used for personally identifiable information.

Security of the servers

- Castor applications run on fully managed virtual private servers, operated on Microsoft Azure.
- All hosting platforms are certified for or compliant with relevant certifications (ISO27001, ISO9001) and/or national or international standards (HIPAA, NEN7510).
- Our servers are patched with security updates on a daily or weekly basis depending on the environment. Critical updates are applied regularly to mitigate potential vulnerabilities.
- Weekly networking vulnerability scans are conducted against all infrastructure.
- Access to data centers is restricted to authorized personnel only. Locations are protected by digital surveillance equipment.
- Backups are made twice daily and stored encrypted within a different physical location to ensure maximum security and continuity.

Server management, security and access control

Castor applications run on fully managed virtual servers on Microsoft Azure in the following regions:

- EU: region EU West (Netherlands) and EU North (Ireland)
- UK: region UK South (London) and UK West (Cardiff)
- AU: region Australia East (New South Wales)
- US: region US East (Virginia) and US West (California)

The providers are responsible for the operations and security of all Castor's hardware up to the hypervisor level. They are responsible for (security) upgrade management and upgrades of the hypervisors, network equipment, data centers, etc.

Security of the network

- All of Castor's applications run on security-hardened servers or containers with only necessary services and ports open to the outside world.
- Web traffic is only permitted using modern, industry standard encryption (>TLS 1.2 and newer), and all uses of cryptography are regularly reviewed.
- Network security groups and firewalls ensure that no unauthorized connections can be made to any of our servers.
- DDoS protection is provided via Microsoft Azure's services.
- Database servers and other data stores are never directly accessible from the public Internet in order to prevent external attacks.

Organizational and Personnel security

- Access to the office is restricted via personal, digital key tags. Visitors have to be accompanied at all times.
- All laptops, phones and other devices used by employees and contractors are fully encrypted.
- Laptops are protected with endpoint security, including anti-virus and anti-malware.
- Passwords and other digital credentials are securely stored within a corporate password manager and access to critical systems requires Multi-Factor Authentication (MFA, also known as 2FA).
- All employees and contractors attend security training every quarter.

Other

In the event of a data breach

At Castor, we do everything in our power to protect your data. If a security breach should occur, we will act quickly to mitigate the damage and keep you informed of the possible implications.

Development

Our Secure Development Procedure describes the software development life cycle and all the measures we take to ensure the best possible security. This includes our release cycles, feature and bugfix procedures, code review requirements and QA processes.

Continuity

All application infrastructure is provisioned in redundant configurations, so that failure of single components can never lead to downtime. Castor has business continuity plans in place to ensure its operations can continue in case of large scale incidents. We execute yearly disaster recovery test procedures in order to ensure that our continuity plans also work in practice and that personnel is trained in their execution.

If anything unexpected should happen to our company itself, we want to minimize the impact this has for our clients. Therefore we provide coverage on the short and long term:

- Short-term coverage through a continuity solution: we have deposited funds in a separate legal entity to ensure hosting continues for at least 3 months, with Castor covering costs for the first month. Long-term coverage through a Source Code Escrow: clients have the option to become a beneficiary of the application source code in the event of bankruptcy or product discontinuation. The code can be deployed in your own environment, or our hosting provider can continue the services. Please contact us if this option interests you.

User responsibilities

You can contribute to the security of your data. We advise everyone not to store patient-identifiable information (surnames, social security numbers, postal codes, date of birth, etc.) within Castor, unless using our Encryption Module.

We also recommend that you follow these best practices when it comes to securing your account and workstation.

Questions?

If you have any questions about the security of Castor, please contact us.

Last updated on August 2024.