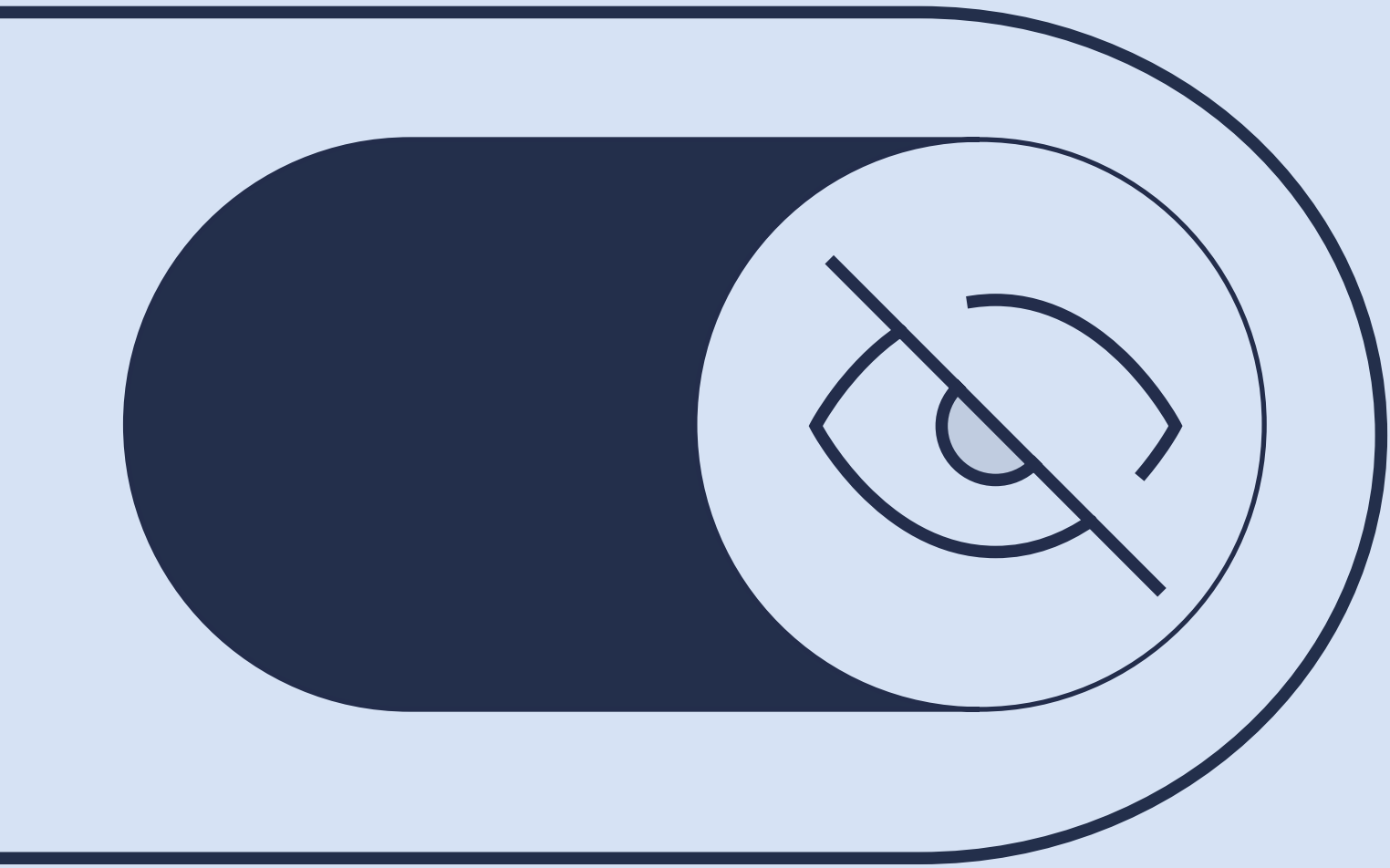
SENBEE

Whitepaper

v2.0 · September 2026

Security at Senbee

An overview of how Senbee protects customer data, manages information security, and secures our smart space platform.



Before we start...

Senbee connects people, spaces and services in one platform. Protecting the information behind these interactions is an essential part of how we develop and operate our services.

This whitepaper outlines our approach to information security, the measures we use to protect customer data, and the responsibilities we share with our customers.

Written by

Tristan White

CEO, Partner

Protecting your data is our top priority

Senbee's information security programme is led by CEO Tristan White. Through our work with ISO/IEC 27001:2022, we take a structured approach to identifying risks, protecting customer information and improving our security practices.

ISO/IEC 27001

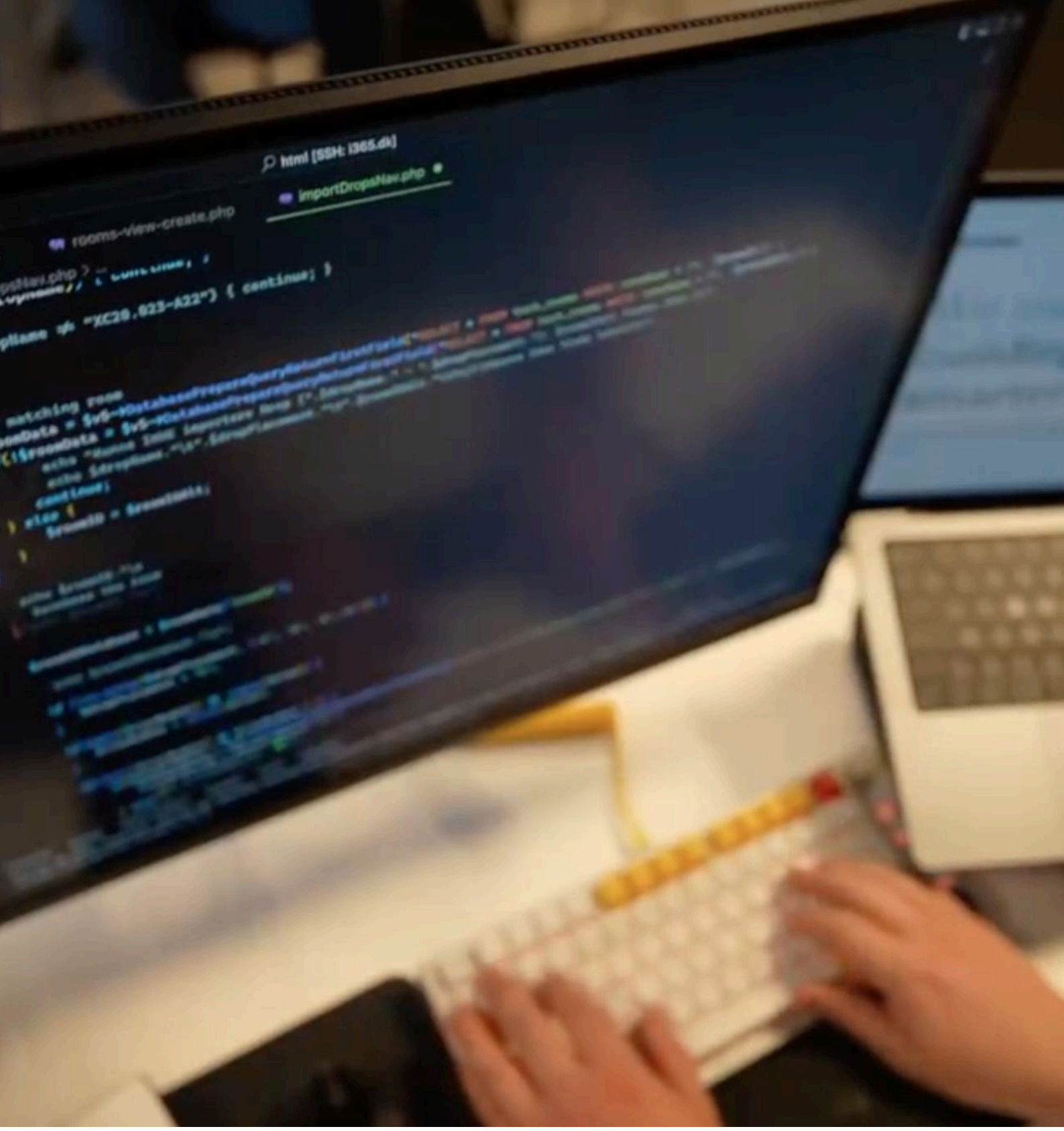
Senbee maintains a comprehensive compliance program that includes third-party assurance. Customers may request access to Senbee's ISO/IEC 27001:2022 certification, and other documentation via our Compliance Portal at **senbee.com/legal**.

Security Reviews

Senbee continuously monitors and improves the effectiveness of its information security controls. We undergo regular internal audits and partner with independent assessors for external audits. All audit results and nonconformities are reviewed by executive management in accordance with our ISMS governance process.

Penetration Testing

Senbee engages an independent security firm to perform annual penetration tests of our networks and applications. All findings are documented, risk-rated, and tracked to resolution. Summary results and remediation progress are reported to senior management.



Senbee’s responsibility

How we protect your data and operate our platform securely

Access control

Senbee enforces access control based on the principles of least privilege and role-based access control (RBAC). Employees are granted only the minimum access necessary to perform their job functions. Access to production infrastructure and critical systems requires multi-factor authentication (MFA).

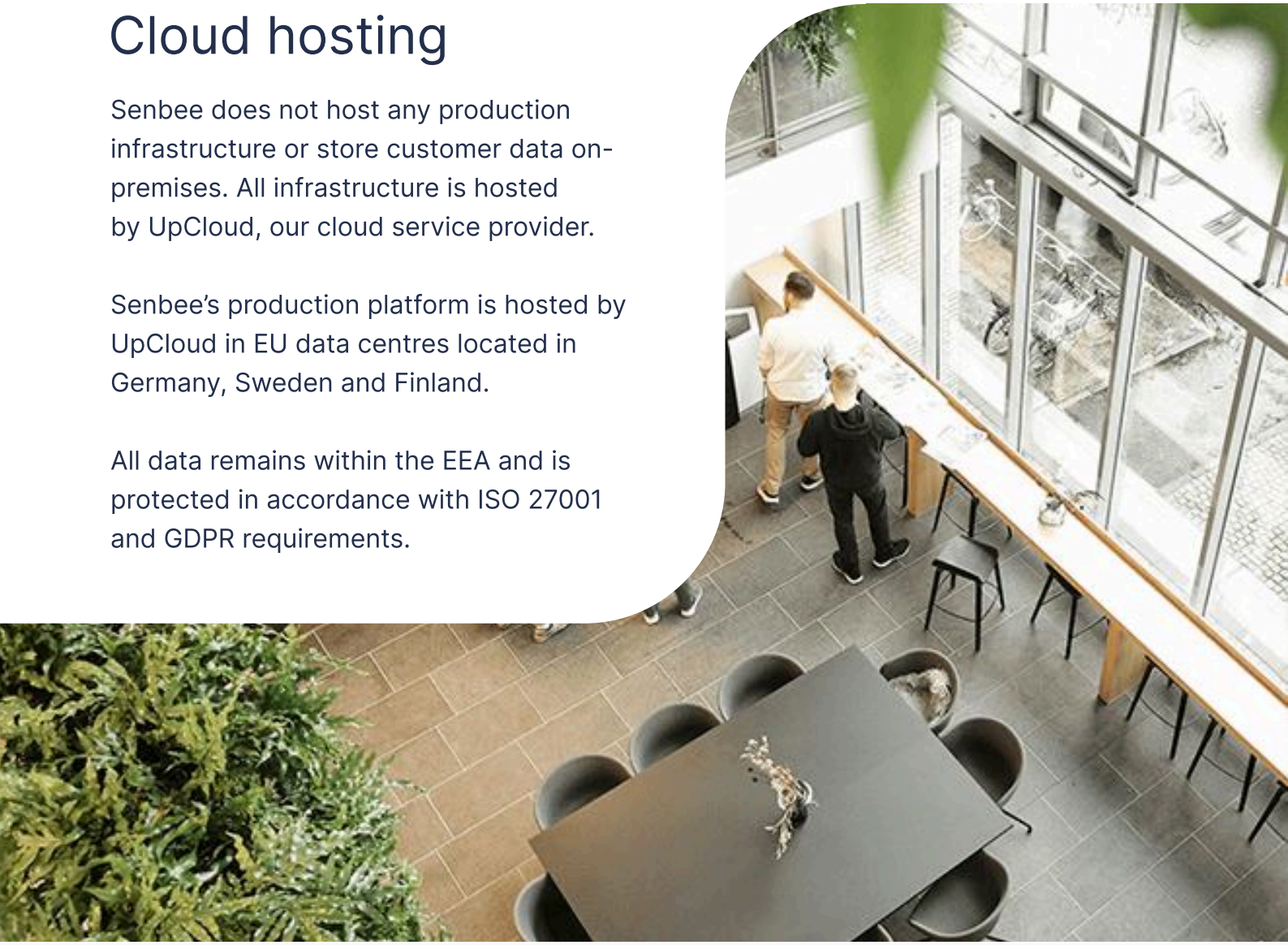
User access reviews are conducted semi-annually, including verification of privileged accounts and production access, in line with our ISMS controls.
Access is revoked at the effective time of an employee's departure, or earlier where required based on risk.

Cloud hosting

Senbee does not host any production infrastructure or store customer data on-premises. All infrastructure is hosted by UpCloud, our cloud service provider.

Senbee's production platform is hosted by UpCloud in EU data centres located in Germany, Sweden and Finland.

All data remains within the EEA and is protected in accordance with ISO 27001 and GDPR requirements.



Data retention

Senbee's backup policy requires encrypted backups of company-managed systems, including servers and databases. Daily backups are retained for 7 days, weekly backups for 28 days, and monthly backups for 12 months. Backup logs are reviewed weekly, and backup and recovery capabilities are tested annually. Reviews and tests are documented to support ongoing improvement and audit activities.

Our hosting provider, UpCloud, is responsible for ensuring the proper sanitization of disks and physical media. Senbee sanitizes employee laptops prior to reuse or disposal.

Encryption

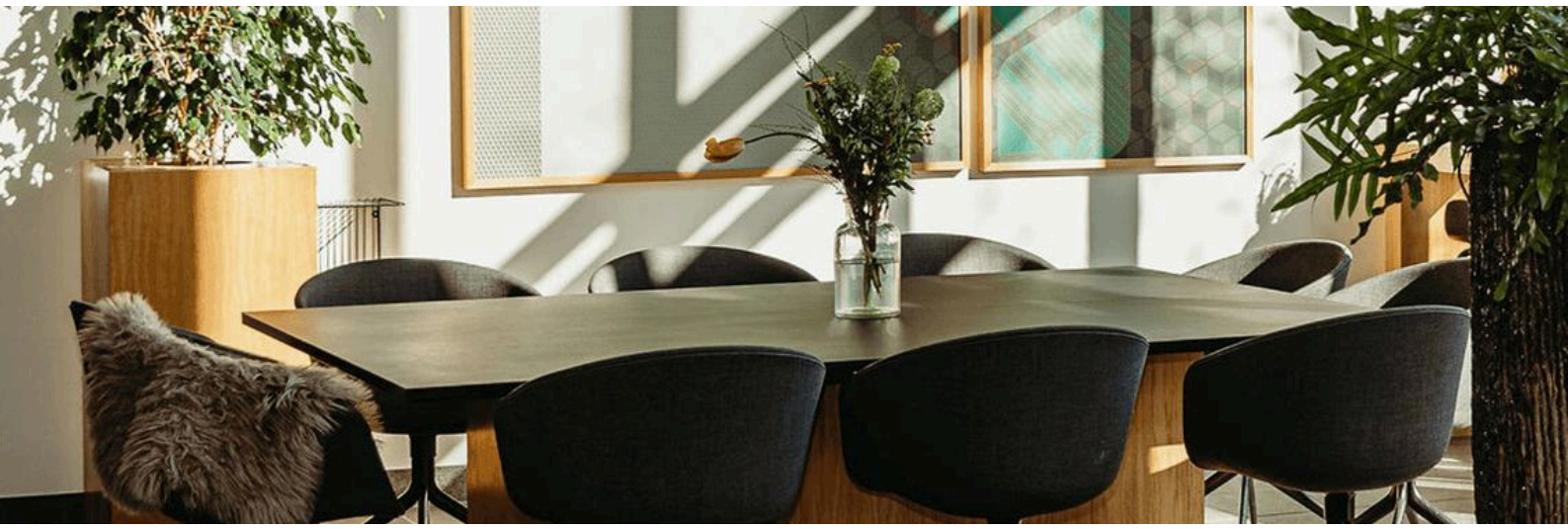
Customer data is encrypted in transit using TLS 1.2 or later and at rest using AES-256 encryption. Database connections are also encrypted using TLS.

Encryption keys are protected through restricted access and managed according to our cryptographic controls.

Logging and Monitoring

Senbee maintains centralized logging for all production systems. Logs are continuously collected and monitored for indicators of compromise or abnormal activity. Automated alerts are triggered when thresholds are exceeded.

Designated personnel review security alerts, investigate suspicious activity and track incidents through to resolution in accordance with Senbee's Incident Response Plan. Significant incidents are escalated to senior management.



Network Security

Senbee firewalls are configured with a default-deny policy for incoming traffic. Firewall rules are reviewed at least annually. Alerts from our Intrusion Detection System (IDS) are routed to on-call personnel for investigation and triage.

A Web Application Firewall (WAF) and Content Delivery Network (CDN) are used to mitigate common web application threats, including DDoS attacks, and to optimize platform performance.

Personnel

Security is a shared responsibility for all Senbee employees and contractors with access to our systems. Personnel are required to accept confidentiality obligations and acknowledge the security policies relevant to their roles.

All employees complete security awareness training during onboarding and annually thereafter. Topics include phishing, remote work, device security, and incident reporting. Developers receive additional training on secure coding practices.

Secure development

Senbee follows a secure software development lifecycle that includes peer code reviews, automated testing and controlled deployment processes. Changes are managed through documented procedures, including provisions for hotfixes and emergency updates.

All code is stored in a version-controlled repository with branch protections. Senbee employs both Static (SAST) and Dynamic (DAST) Application Security Testing. Access to source code requires multi-factor authentication (MFA).

Third parties

Senbee partners with third parties to deliver core services. Sub-processors that handle customer personal data are monitored to ensure their security practices meet Senbee's requirements.

Each sub-processor is reassessed annually, including a review of their audit reports, certifications, and penetration test results. For a current list of approved sub-processors, visit senbee.com/legal/sub-processors.

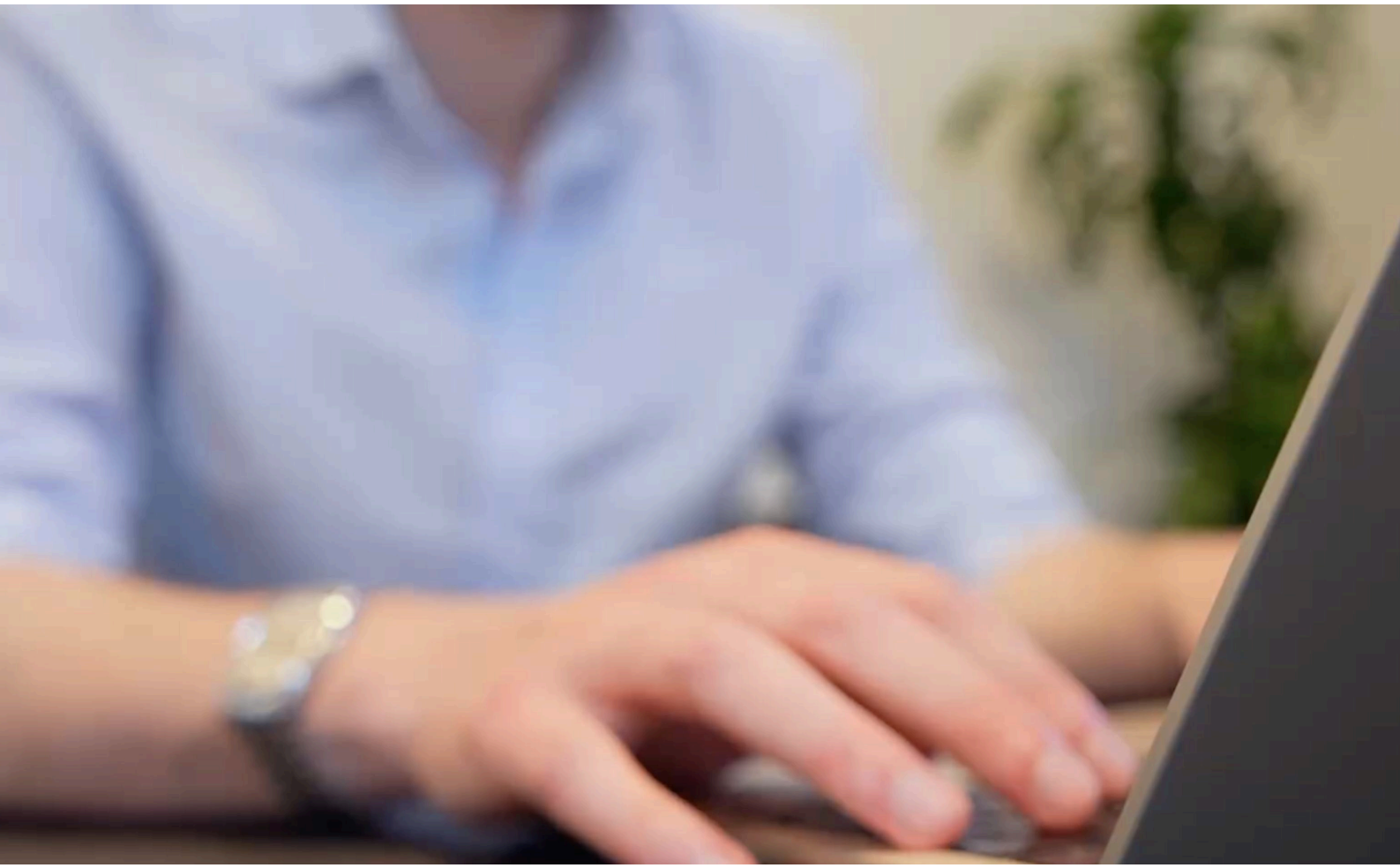
Vulnerability management

Senbee conducts internal and external vulnerability scans weekly. Findings are triaged and remediated based on severity and potential impact, following defined SLAs.

Your responsibility

Customers are responsible for managing their users and assigning appropriate permissions. This includes protecting login credentials, reviewing access regularly and promptly removing access when it is no longer needed. Where available, customers should enable multi-factor authenticatio

The information processed by Senbee depends on the services and integrations a customer uses. Customers are responsible for ensuring that the data they enter or connect is appropriate for the agreed service and that access is limited to authorised users. Sensitive personal data and payment card details should only be submitted where explicitly supported and agreed with Senbee.



Security is part of how we work

Protecting customer information is an ongoing commitment at Senbee. We continually review and improve our security practices as our platform, customer needs and risks evolve.

For questions about our security practices or to request supporting documentation, please contact us.

Want to get in touch?

+45 93 200 555

hello@senbee.com

Åbogade 15,
8200 Aarhus N, Denmark