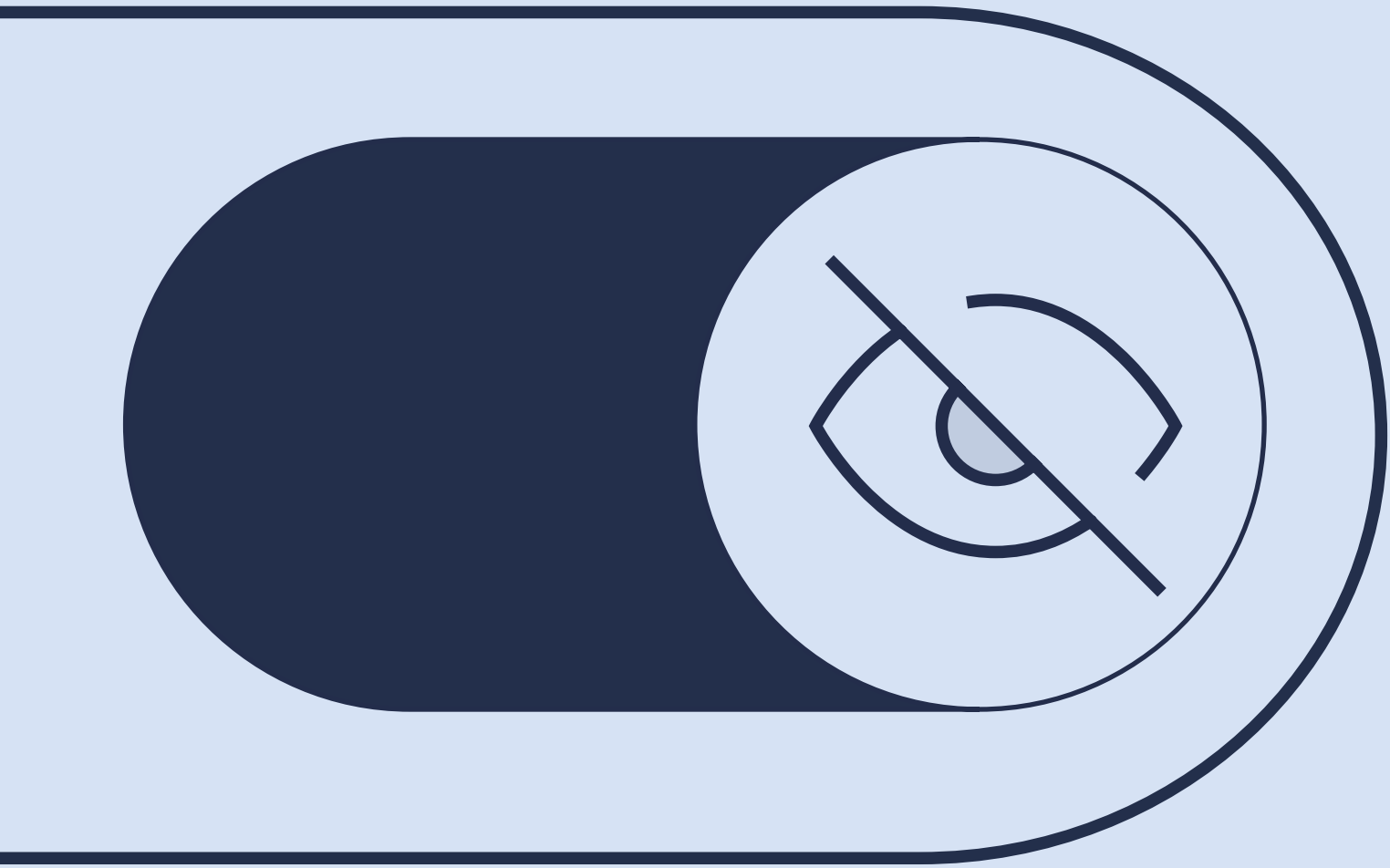
SENBEE

Whitepaper

Security at Senbee

The technology and systems behind our enterprise-ready smart space platform, and exactly how Senbee ensures the security and privacy of your data.



Before we start...

Senbee places people at the heart of building interaction, automating and optimizing every aspect of how they experience a space for a smarter, more secure and more intuitive environment.

This whitepaper highlights our security practices to help you understand how we ensure security by design.

Written by

Tristan White

CEO, Partner

Protecting your data is our top priority

Senbee's security program is led by our CEO, Tristan White, and managed by a dedicated security team. The program is designed to prevent unauthorized access, use, and disclosure of customer data. It aligns with the ISO/IEC 27001:2022 standard and is informed by the AICPA Trust Services Criteria. Our controls and practices are continuously improved based on evolving risks and industry best practices, ensuring security is embedded across all levels of the organization.

Independent Attestation

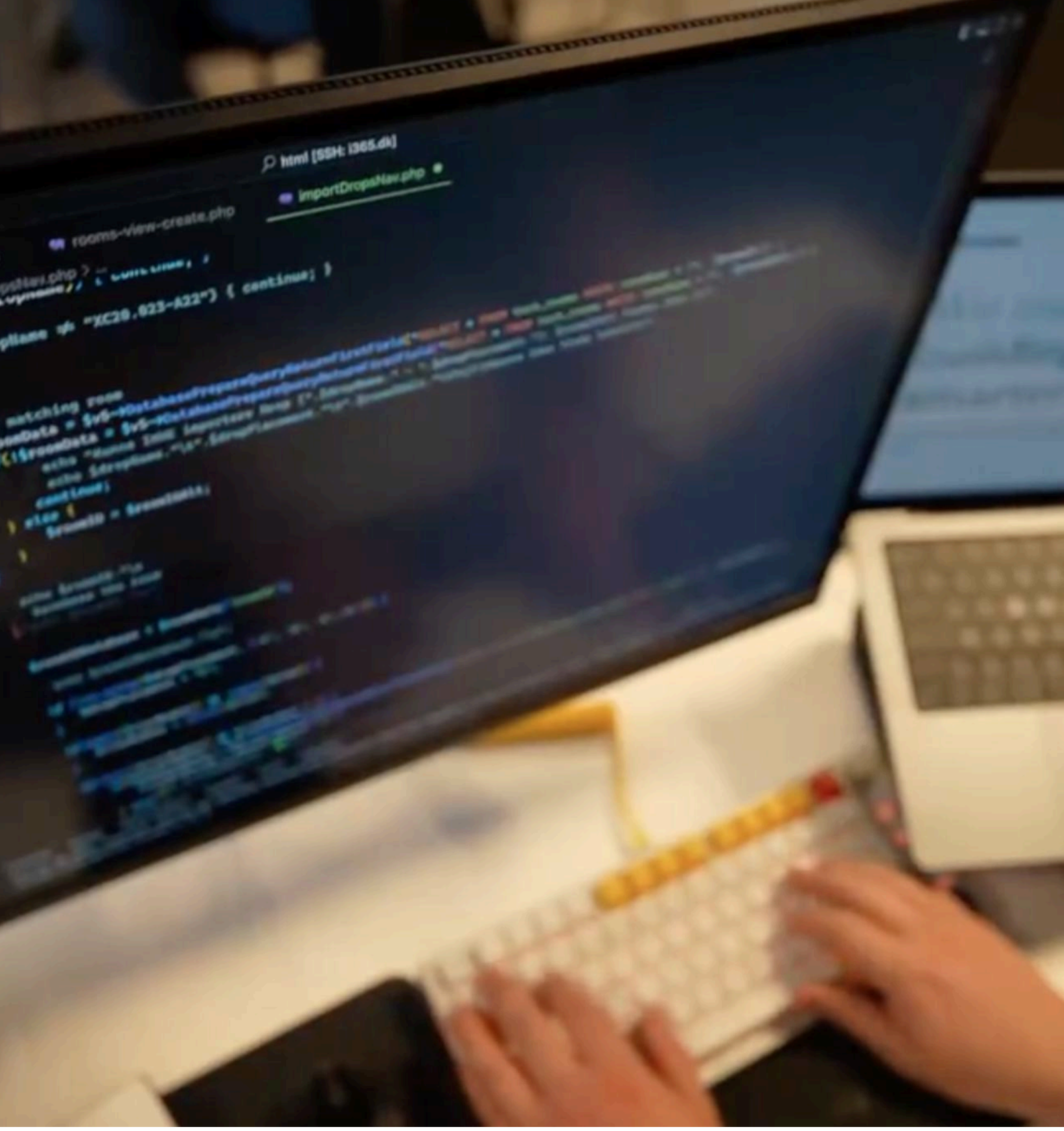
Senbee maintains a comprehensive compliance program that includes third-party assurance. Customers may request access to Senbee's ISO/IEC 27001:2022 certification, and other documentation via our Compliance Portal at **senbee.com/legal**.

Security Compliance

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

Policies & practices for protecting your data

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).

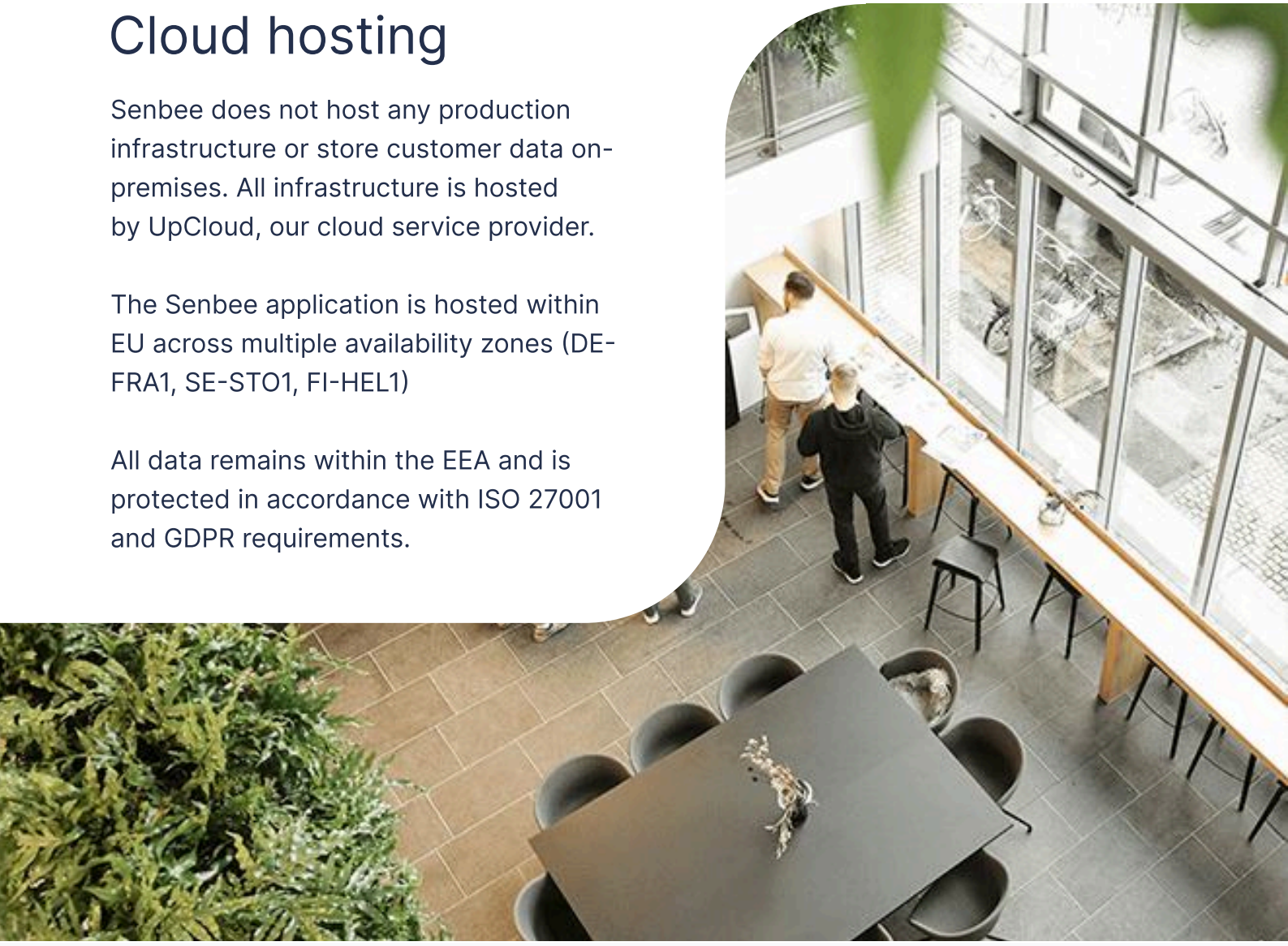
User access reviews are conducted semi-annually, including verification of privileged accounts and production access, in line with our ISMS controls.
Access is revoked immediately upon involuntary termination. For voluntary terminations, access is removed within two business days.

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.

The Senbee application is hosted within EU across multiple availability zones (DE-FRA1, SE-STO1, FI-HEL1)

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



Data retention

Senbee retains customer data for the duration of the service agreement. Upon termination, data is retained in accordance with Senbee's Data Retention Policy, unless a written deletion request is received from the customer.

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

Senbee encrypts all customer data at rest and in transit using strong encryption methods. All information is transmitted via HTTPS using TLS1.2+ with AES256 encryption and SHA2 signatures, defaulting to TLS1.3 based on client capability.

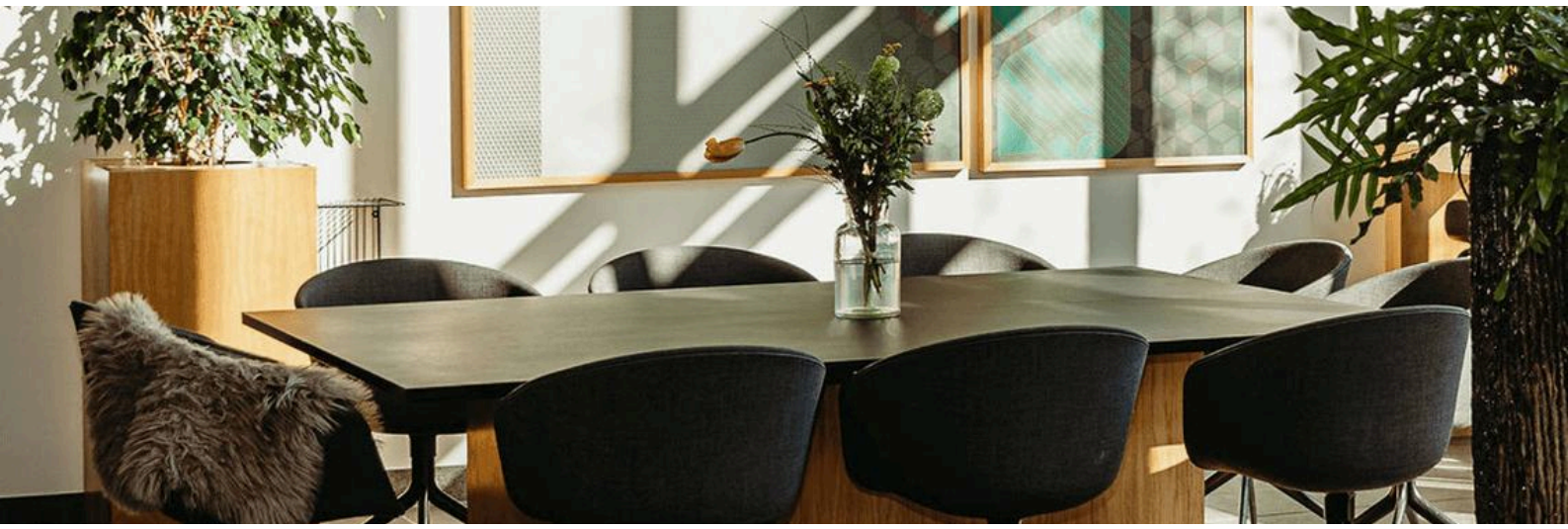
Data at rest is encrypted at the storage level using AES256. Database connections are verified using TLS certificates and encrypted in transit using SSL.

Encryption keys are managed and stored securely by UpCloud. Senbee personnel do not have access to the encryption keys. All key usage is logged and monitored for anomalous activity.

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.

The Security team is responsible for reviewing logs, responding to alerts, and tracking security events through to resolution. All activities are handled in accordance with Senbee's Incident Response Plan, and 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 at Senbee is a shared responsibility of all employees and contractors with access to our systems. Before starting, individuals must pass a background check (where legally permitted) and sign a confidentiality agreement, the employee handbook, and Senbee's security policies.

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.

Policy violations may result in disciplinary action, up to and including termination.

Secure development

Senbee follows a secure software development lifecycle (SDLC) that includes peer code reviews, automated testing, and change management for non-standard updates, including hotfixes and emergency changes. Our agile workflow supports continuous delivery, allowing engineers to deploy improvements independently.

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.

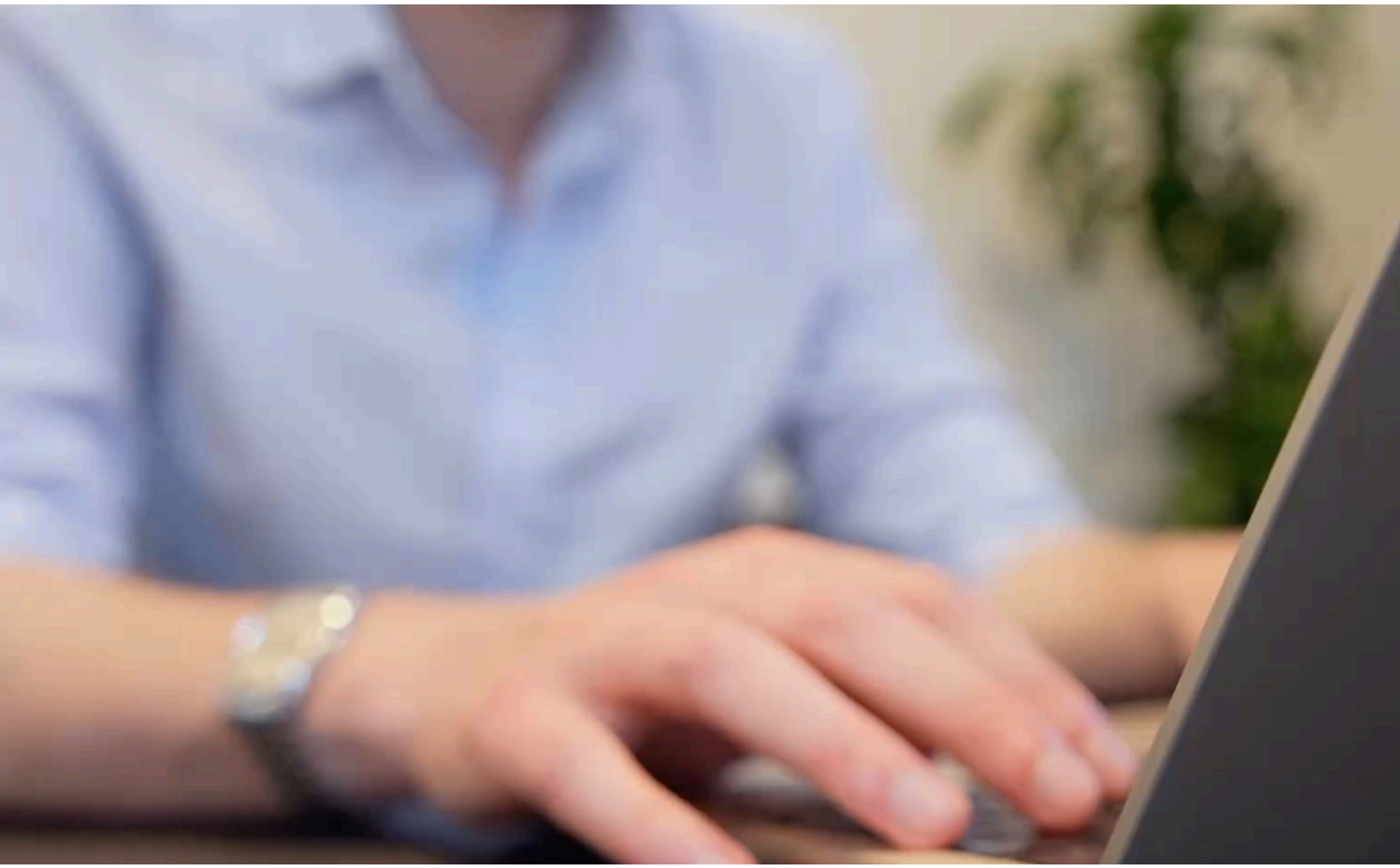
Each sub-processor is reassessed annually, including a review of their audit reports, certifications, and penetration test results. For a current list of approved sub-processors, visitsenbee.com/legal/sub-processors.

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

Your responsibility

While Senbee manages the security of the platform and underlying infrastructure, customers are responsible for securing their own user accounts. This includes using strong passwords, managing account provisioning and permissions, and deactivating accounts when no longer needed.

Customers are also responsible for the type of data they enter into the platform. By default, Senbee only processes limited personal data (e.g., name and email). Customers should avoid inputting sensitive or regulated data such as cardholder information or protected health information, unless explicitly agreed upon.



Ensuring security & privacy of customer information is part of our mission

Ensuring the security and privacy of customer information is essential to our mission at Senbee. The success of our customers is at the heart of everything we do.

We hope this overview of our security program helps to build and maintain your trust in Senbee.

Want to get in touch?

+45 93 200 555

hello@senbee.com

Åbogade 15,
8200 Aarhus N, Denmark