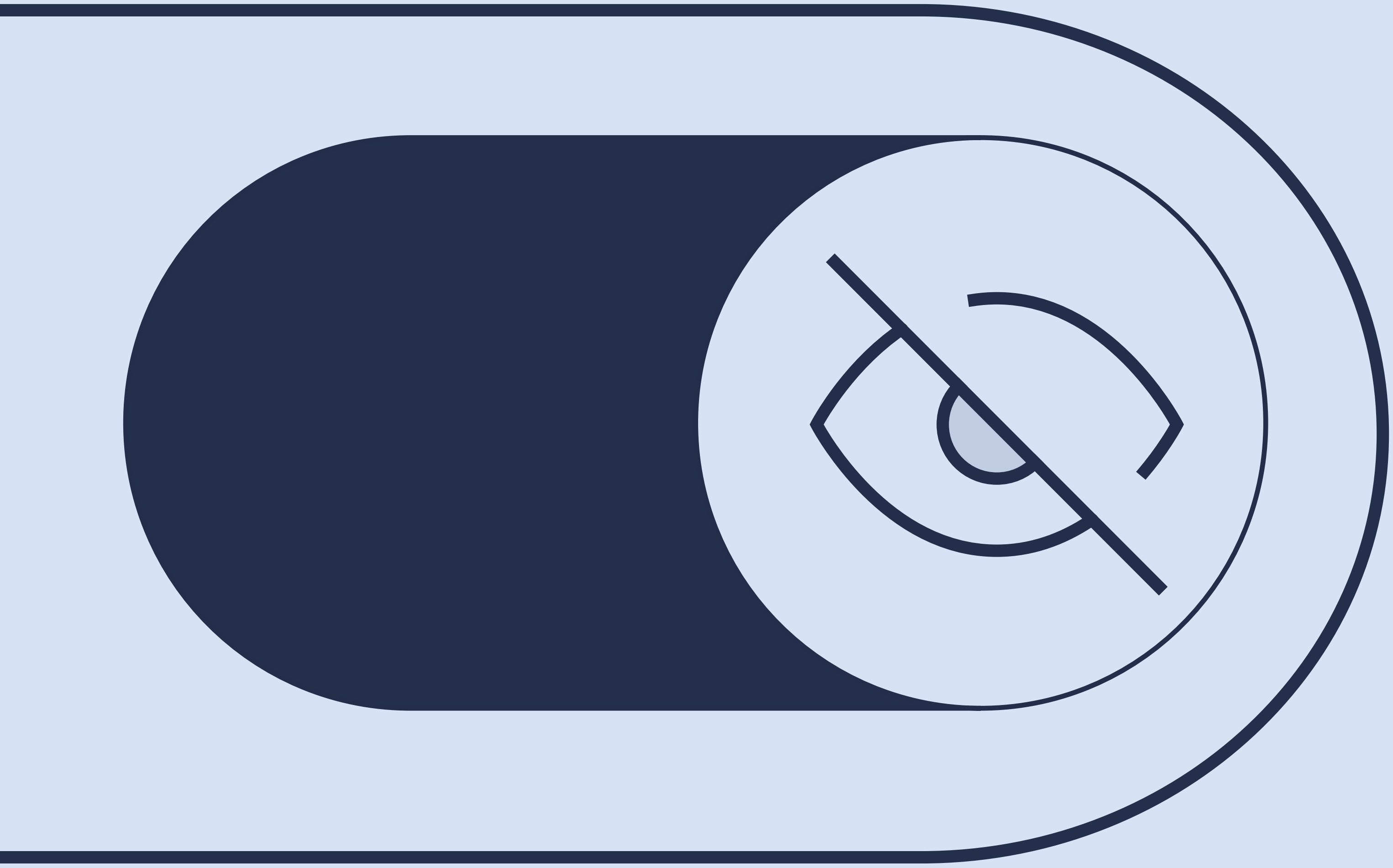
SENBEE

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 team, led by our CEO, Tristan White, is responsible for implementing and managing our security program. The focus of Senbee's security program is to prevent unauthorized access, use, and disclosure of customer data. Our program is aligned with AICPA Trust Services Principles and continuously evolves in accordance with industry best practices, ensuring security is taken seriously from top to bottom.

Independent Attestation

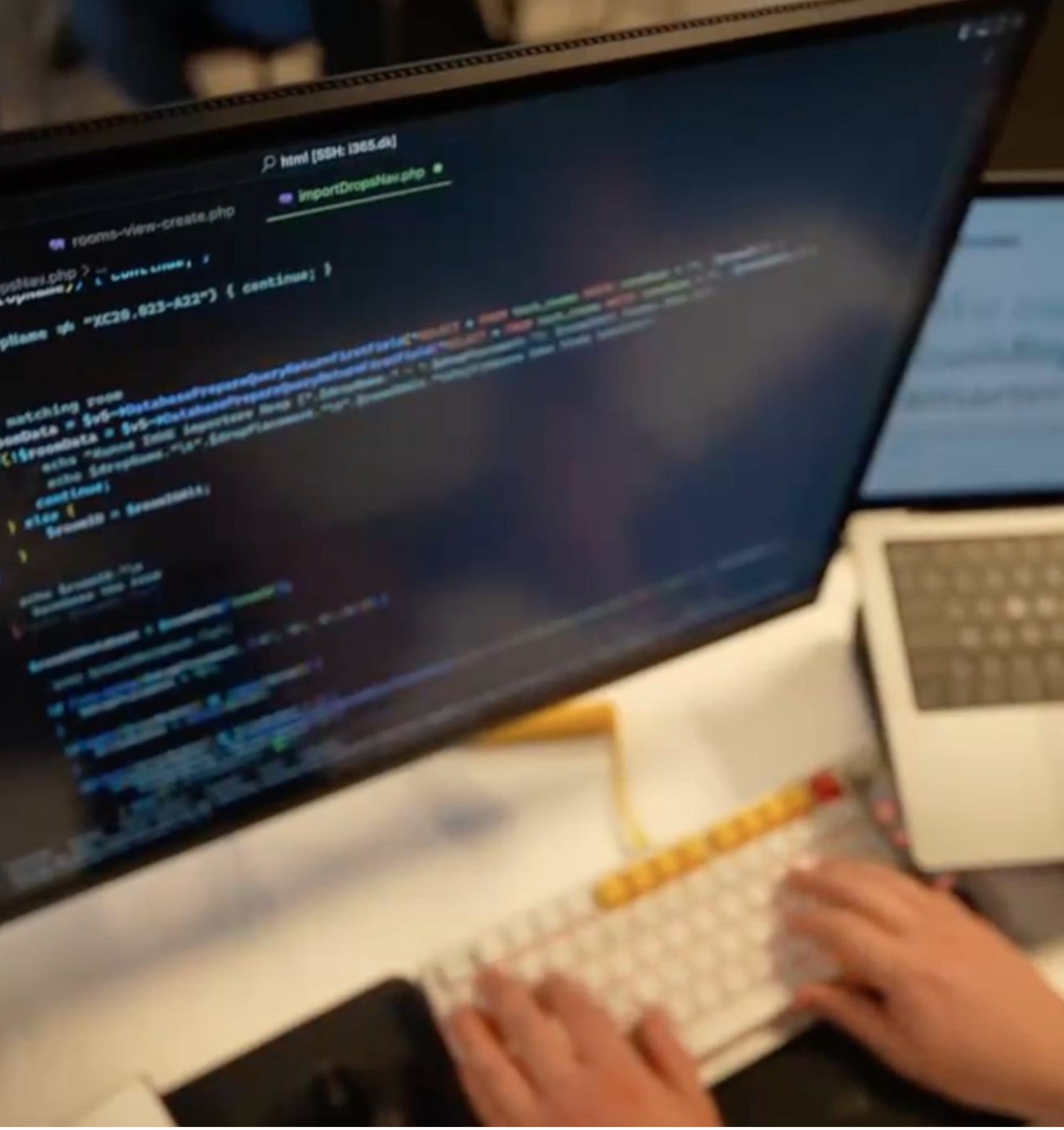
Customers may receive copies of Senbee's SOC2 report, as well as all other available documentation from our Compliance Portal at **senbee.com/legal**

Security Compliance

Senbee continuously monitors and improves the design and effectiveness of our security controls. We partner with a reputable third party for independent assessments of our efforts. All internal and external audit findings are shared with executive management.

Penetration Testing

Senbee engages an independent third party to conduct annual network and application penetration tests. Identified findings are tracked to resolution, and result reports are shared with executive management.



Senbee’s responsibility

Policies & practices for protecting your data

Access control

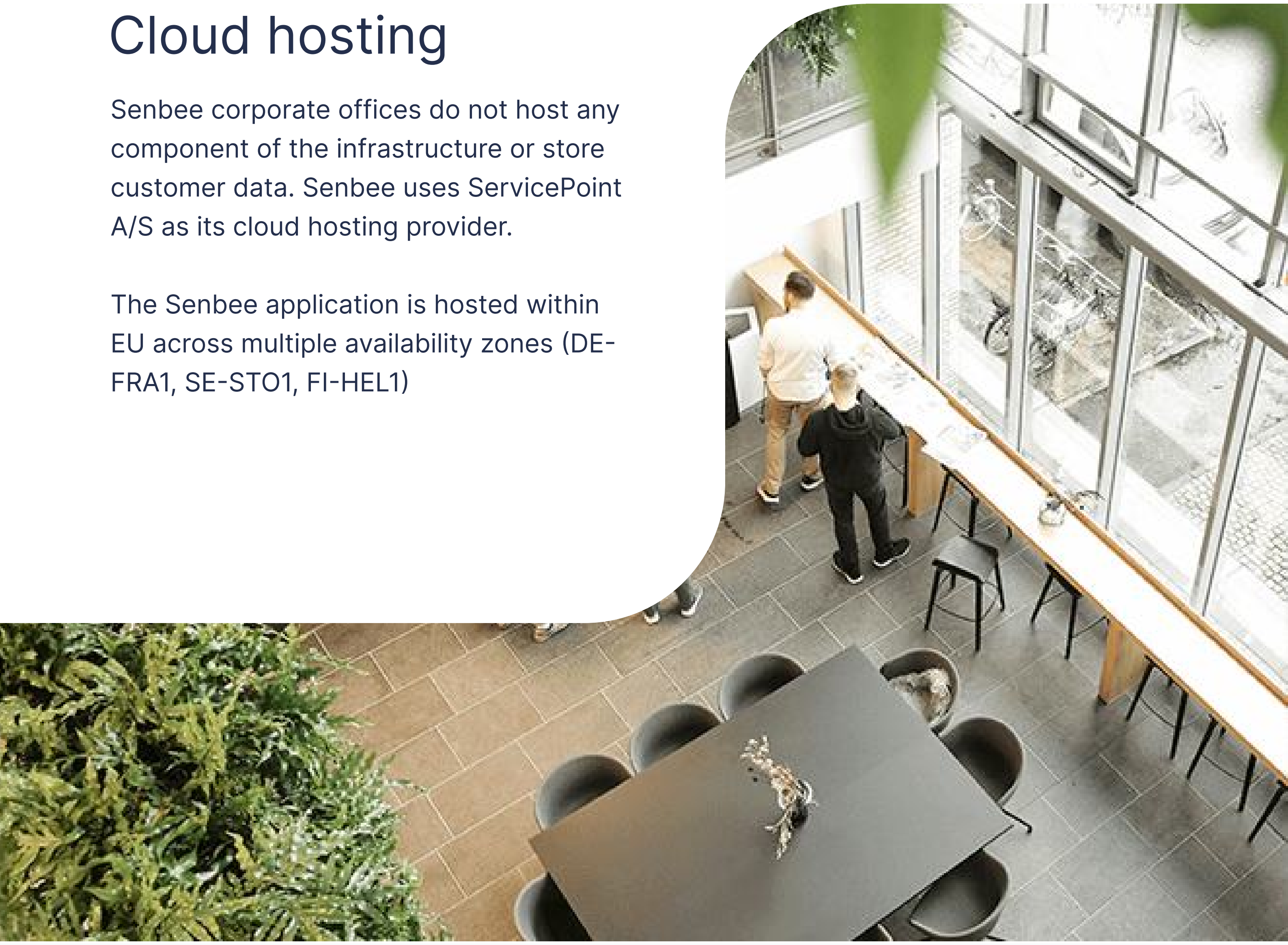
When provisioning access, IT adheres to the principles of least privilege and role-based access control, meaning that employees are only authorized the access and permissions required to fulfill their job responsibilities. User access reviews, including production access, are performed semi-annually. Access to the production infrastructure and supporting systems requires MFA.

Employee access is revoked within two business days of an employee’s termination. In the event of involuntary termination, access is revoked immediately.

Cloud hosting

Senbee corporate offices do not host any component of the infrastructure or store customer data. Senbee uses ServicePoint A/S as its cloud hosting provider.

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



Data retention

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

Our hosting provider, ServicePoint A/S, 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 ServicePoint A/S. Senbee personnel do not have access to the encryption keys. All key usage is logged and monitored for anomalous activity.

Logging and Monitoring

Centralized logging is enabled for all production systems at Senbee. These logs are reviewed for signs of compromise and generate alerts. The Security team is responsible for monitoring and responding when alert thresholds are reached, tracking security events to resolution in accordance with the incident response plan.

Network Security

Senbee’s firewalls are configured to deny all incoming traffic by default. Firewall rules are reviewed at least annually. Alerts generated by the Intrusion Detection System (IDS) are sent to on-call personnel for investigation and triage. Senbee also utilizes a Web Application Firewall (WAF) and Content Delivery Network (CDN) to protect against common web application vulnerabilities, such as DDoS attacks, and to provide faster access to the platform.

Personnel

Security of the Senbee environment is the shared responsibility of all Senbee employees and contractors who have access to our information systems. Prior to their start date, all employees and contractors must have a completed background check on file, as legally permissible. Employees and contractors must also sign a confidentiality agreement, the employee handbook, and Senbee’s security policies.

All employees are required to complete security awareness training upon hire and annually thereafter. The training curriculum includes phishing awareness, remote work best practices, device security, and incident reporting. Developers are required to complete additional training focused on secure coding practices.

Violations of any corporate policies may result in disciplinary action, up to and including termination.

Secure development

Senbee has established a secure software development lifecycle (SDLC) that includes requirements such as independent peer code review and automated testing. Non-standard changes go through a change management process that accounts for emergency changes and hotfixes. The agile nature of the process allows engineers to follow their own release cycles, deploying continuous improvements to the Senbee platform.

All code is managed in a version control repository with branch protections in place. Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) are also implemented. Access to source code requires multi-factor authentication (MFA)

Third parties

Senbee partners with third parties to provide key services. Third parties that handle customer personal data, also known as sub-processors, are continuously monitored to ensure their security programs meet Senbee's standards. Senbee reassesses its sub-processors annually, which includes a review of their independent audit reports and penetration test results. For the full list of Senbee's sub-processors, please visit senbee.com/legal/sub-processors.

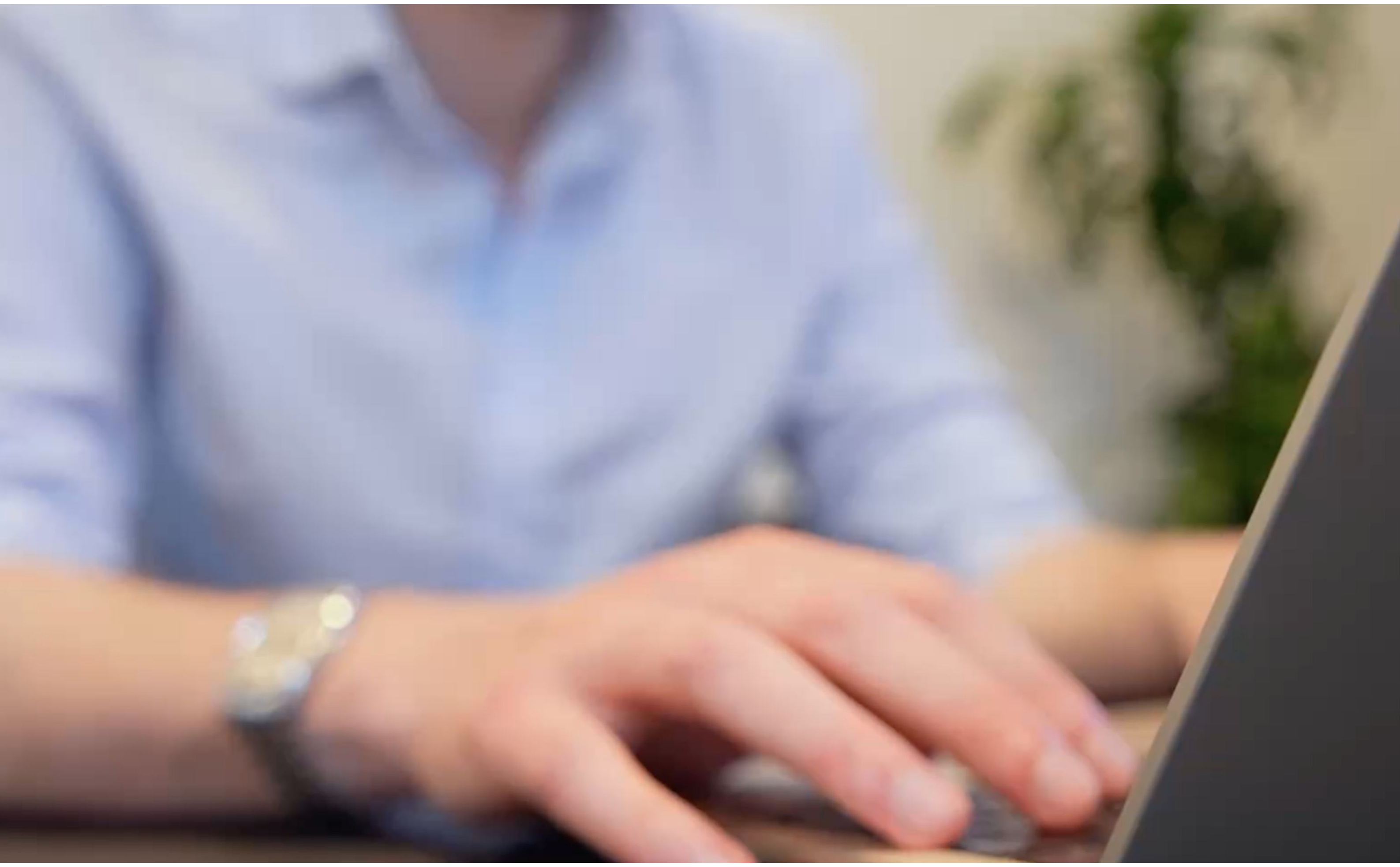
Vulnerability Detection

Senbee performs internal and external vulnerability scans on a weekly basis. Identified vulnerabilities are remediated according to their severity.

Your responsibility

While Senbee is responsible for the majority of security controls that protect customer data and the platform, our customers are responsible for securing their user accounts. This includes creating strong passwords, managing user account provisioning and permissions, and disabling accounts when necessary.

Additionally, customers are responsible for determining the appropriateness of the data entered into the platform. By default, Senbee handles limited customer PII (name and email). The sensitivity of the data customers input into the system is ultimately their responsibility. Customers should avoid submitting cardholder information, protected health information, and other types of sensitive, regulated data.



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