accessiBe

Security and privacy statements

Are you wondering about accessiBe’s security? Here are some FAQs to help.

accessiBe Ltd. is a limited liability company incorporated in Israel and is the parent company of accessiBe Inc. accessiBe’s products and services are built with the belief that every business, regardless of size, budget, and resources, should strive to incorporate accessibility principles, endorse inclusion, and treat all customers (with or without disabilities) equitably and respectfully, and should have access tools to practicably achieve these goals. In accordance with this belief, accessiBe has developed an ecosystem of solutions for businesses of all sizes to achieve and maintain accessibility throughout their software lifecycle and to incorporate accessibility into the core of their web projects. accessiBe currently offers three web accessibility products: accessWidget, accessFlow, and accessScan, as well as a professional services department.

What type of information does accessiBe handle?

We collect various types of information, including Personal Information, when a Customer or a Visitor (including anyone acting on their behalf) accesses or uses our Services as more fully set forth in our Privacy Notice - link

What is your Security and Privacy Mission?

The role of the information security program, as defined by accessiBe’s management, is to provide the continuous improvement guideline for organizational security and privacy controls to support accessiBe’s Security Vision. In order to accomplish this mission statement, accessiBe‘s management leads and builds its security and privacy organization. This organization will drive the following missions:

1. Protect corporate and client data
2. Drive accessiBe’s governance, risk, and compliance in relation to security and privacy
3. Maintain a high level of security and privacy controls’ maturity
4. Develop a foundation for a forward-thinking and proactive security approach

accessiBe’s security team periodically assesses the sufficiency of its information systems to capture and report data that is timely, current, accurate, and accessible. For high-severity incidents, Root Cause Analysis (RCA) is performed through various tools and meetings in order to improve the quality of the solution accessiBe provides to customers.

Service Level Agreements (SLA) with third parties exist and include monitoring the process and the access (as applicable).

Are penetration tests conducted periodically to identify weaknesses and vulnerabilities in the IT infrastructure?

Penetration tests are conducted on an annual basis. Findings are mitigated according to their severity and accessiBe's work plan.

Does accessiBe have a dedicated team responsible for overseeing and managing security?

accessiBe’s Security& IT team is responsible for all security aspects, including:

1. Comply with relevant legal and regulatory requirements to ensure that statutory obligations are met, clients’ expectations are managed, and civil or criminal penalties are avoided.
2. Adopt a risk-based approach to ensure that information security risks are treated in a consistent and effective manner.
3. Ensure that information security is integrated into essential business activities.
4. Keep up to date with changing security threats.
5. Mitigate information security risk to a manageable level that is accepted by accessiBe’s senior management.
6. Maintain adherence to legislative requirements, regulatory requirements, and audit recommendations.
7. Meet the operating needs of the organization securely.

What policies and procedures are in place to ensure the security of sensitive data and information?

accessiBe has written, approved by the management, and implemented security policies & procedures in order to adhere to the security program according to SOC2 and ISO27001 standards.

Is there an awareness training program in place to educate staff on how to secure information and systems?

Users (including employees and contractors) are the first and most important line of defense against security threats. It is, therefore, essential that they are educated on security issues related to their job. accessiBe's awareness program includes onboarding frontal training, a dedicated awareness communication channel, and Phishing campaigns conducted throughout the year.

How does accessiBe monitor and detect unauthorized access or suspicious activity?

accessiBe has deployed various tools and services in order to protect accessiBe’s cloud environment and IT assets against outsiders and threats to the system’s security. These controls are monitored by the Security Team, and unusual activity is researched and resolved, in addition to pre-defined events. The company reviews logs of security events for security exceptions and inappropriate user activities on a regular basis and implements automated alerts to identify and respond to security issues.

How will customers be notified in the event of a security incident?

Clients and business partners will be notified at various stages of disaster recovery using email and our official status page based on the terms of use agreement. If these methods are unavailable, notification will happen via alternative means (cell phone, etc.) as provided by each client.

How does the company ensure compliance with relevant security regulations and standards?

accessiBe is certified with SOC2 Type2 and all policies and procedures are aligned with security frameworks such as ISO27001 & ISO27701.

Does the company have a formal process for reviewing and approving cloud-based applications and services before they are used by employees or customers?

To ensure compliance with SOC2 and ISO27001 standards, we have implemented a vendor management program that includes due diligence, risk assessment, and ongoing monitoring of all third party systems and vendors with access to our sensitive information. This program requires all vendors to comply with our information security policies and controls, access controls, and incident response procedures. Additionally, we conduct periodic security assessments of all third-party systems and vendors to ensure they continue to meet our security standards and mitigate any potential risks.

Is there a risk management plan in place?

Risk management in the company includes all aspects of information security deployment, including policy, information security procedures, and all other relevant activities. Risk management is an ongoing process; therefore, all activities related to risk management will be conducted on a periodic and routine basis. The company defined the ISO 27005 standard as its risk management guidelines for all information security-related activities. Information security risk management is an integral part of all information security management activity and is applied both to the implementation and ongoing operation.

Is data and all communication encrypted?

We ensure compliance with SOC2 and ISO27001 standards by encrypting our data at rest using GCP's KMS and with secure key management practices. This includes encryption of all data stored in databases and file systems, as well as secure management of encryption keys through regular rotation and strict access controls. Additionally, for data in motion, we implement SSL/TLS encryption for all network traffic to protect the confidentiality and integrity of information during transmission.

Thank you for your interest in accesiBe’s security.