Information Security Framework

Safeguarding the privacy and confidentiality of data right from the source
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Certifications and compliance</td>
<td>3</td>
</tr>
<tr>
<td>Data privacy and handling</td>
<td>4</td>
</tr>
<tr>
<td>Sensitive data policy</td>
<td></td>
</tr>
<tr>
<td>PII</td>
<td></td>
</tr>
<tr>
<td>PCI</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
</tr>
<tr>
<td>Data storage</td>
<td>5</td>
</tr>
<tr>
<td>Data center security</td>
<td></td>
</tr>
<tr>
<td>Network protection</td>
<td></td>
</tr>
<tr>
<td>Access control</td>
<td>6</td>
</tr>
<tr>
<td>SessionCam account security</td>
<td></td>
</tr>
<tr>
<td>Product updates and testing</td>
<td></td>
</tr>
<tr>
<td>Penetration testing</td>
<td></td>
</tr>
<tr>
<td>Business Continuity Plan (BCP)</td>
<td></td>
</tr>
<tr>
<td>Security culture</td>
<td>7</td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
</tr>
<tr>
<td>Human resources</td>
<td></td>
</tr>
<tr>
<td>Our people</td>
<td></td>
</tr>
</tbody>
</table>
INTRODUCTION

Security is at the heart of SessionCam’s commitment to you. As a SaaS solution provider, we understand that maintaining and protecting the privacy and confidentiality of data is critical to your business. Our high-security standards and practices mean you’ll be in control of the data we record and be kept informed of how we use it.

CERTIFICATIONS AND COMPLIANCE

SessionCam’s security framework is closely aligned with ISO/IEC 27001:2013, the internationally recognized Information Security standard that provides a framework of best practices, policies and procedures that include legal, physical and technical controls involved in an organization’s information risk management processes.

In the UK, we are registered with the ICO, the UK’s independent authority set up to uphold information rights in the public interest in compliance with the Data Protection Act.

You can review our Data Protection Register entry here (DPA registration number: ZA115103).

Peace of mind
Alignment with these world-class standards is designed to protect both the information assets of your business and our own. We are required to continually review potential information security risks and take the appropriate corrective actions to stay one-step ahead and keep your data secure.
SessionCam is committed to ensuring that data is stored, archived or disposed of in a safe and secure manner.

In the interest of transparency, you have complete control over the data we record. Any data recorded and stored by SessionCam on behalf of our customers is exclusively for their own use and is encrypted.

We do not sell, share, rent or exchange any data or information recorded for customers with third-party organizations.

**Sensitive data policy**

For security purposes, fields marked as sensitive won’t be recorded or stored and will appear starred-out, or masked, in playback. Once data has been set to be masked, it will never leave the user’s browser.

Our sensitive data policy can be applied at these levels:

- Whole site
- Individual page
- Input field and page content (HTML)
- Secure data generated within the HTML page

If you do not wish to capture the full IP address of your site visitors for privacy reasons, we can mask the entire IP or any pre-specified number of octets from the IP.

**PII**

SessionCam understands that Personally Identifiable Information (PII) should be accessed only on a strict need-to-know basis, and handled and stored with care.

All our customers are given the option to record PII if they so wish. A common reason for doing so would be as an anti-fraud measure.

**PCI**

SessionCam does not collect Payment Card Industry (PCI) data by default. It is programmed to recognize fields containing PCI data and not record them. As SessionCam is designed to show you customer behavior, it is not necessary to record this sensitive information, so we don’t.

By not recording PII and PCI data, the SessionCam solution does not compromise your compliance with industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA) or national laws relating to PII.

**Encryption**

Data recorded and stored by SessionCam is encrypted using AES-256 encryption. This is the highest Advanced Encryption Standard (AES) and - for example - is used by the US Government to protect classified information.

Every protected object is encrypted with a unique encryption key. This object key itself is then encrypted with a regularly rotated master key. Additional security is provided by storing the encrypted data and encryption keys in different hosts.

Any data recorded by SessionCam from the browser is transferred to our secure environment using SSL/TLS encryption. This is the standard for establishing an encrypted link between a web server and a browser, and it ensures that all data passed between the two points remains private.

Questions? Email support@sessioncam.com or contact your Account Manager for more information.
SessionCam is hosted on Amazon Web Services (AWS S3). Based in the US, all data is held on secure servers.

For customers based in Europe who are concerned about data being stored outside the EU, AWS is not only signed-up to EU Data Protection Regulations, but also ensures compliance with the new EU-US Privacy Shield. Set out in July 2016 as a replacement for the Safe Harbour program, the framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the US.

Data center security
Amazon has proven experience in designing, constructing and operating large-scale data centers. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff, utilizing video surveillance and intrusion detection systems.

The Amazon cloud infrastructure is designed and managed in accordance with major regulations and standards, and complies with the following:

- Payment Card Industry Data Security Level 1 (PCI DSS)
- Service Organization Controls (SOC) 1, 2 & 3
- Health Insurance Portability and Accountability Act (HIPAA)
- ISO 27001 and ISO 9001

A fully comprehensive list of compliances can be found on the AWS website.

Network protection
The Amazon Web Services network offers major protection against traditional network security issues, such as:

- A managed firewall service featuring a combination of products and technologies to protect the live environments
- Distributed denial of service (DDoS) attacks
- ‘Man in the middle’ (MITM) attacks
- IP spoofing: Amazon EC2 instances cannot send spoofed network traffic
- Port scanning: Any unauthorized port scanning stopped and blocked

Questions? Email support@sessioncam.com or contact your Account Manager for more information.
We structure your SessionCam account setup to allow only the users you specify to gain access to each site, or group of sites and the product features necessary for each individual. When logging in, a new user is presented with a default account and only has access to the views of the data they have been authorized to see. You can then assign different user roles which provide access to different features of the SessionCam console.

There are currently four main user access roles: Alert Receiver, Standard User, Analytics User and Admin User. Users can be added and revoked at your request via the SessionCam Customer Success team with a request from your nominated account contact.

SessionCam account security

SessionCam has two public points of entry to the system, the Recording Console and Customer Console. We implement the following security around our login system:

- Logging into the SessionCam Console - whether as a customer or SessionCam employee - is encrypted in transit by default

- Accounts and individual logins are unique and all access is audited
- Passwords have to be a minimum of eight characters in length and include at least one numeric character
- Auto-complete of username and password information in the browser has been disabled
- No passwords are stored in clear text. They are stored as hashes, which means no-one else can read it
- To protect against brute force attacks, your account will be locked out after multiple unsuccessful login attempts and the password will need to be reset by the SessionCam Customer Success Team
- Incorrect login attempts are logged on a per user basis and we keep a timestamp of the last successful login on an account

Product updates and testing

SessionCam has a strict change control process, all releases are extensively tested with a combination of manual and automated testing.

SessionCam performs a monthly vulnerability scan of the solution using a leading industry scanning tool. The scan is also completed after each major release.

Penetration testing

SessionCam conducts an annual external test for vulnerabilities, undertaken by an independent information security company.

We welcome customer vulnerability tests on our solution to give you peace of mind. If you wish to carry out your own test, please contact your account manager or email support@sessioncam.com.

Business Continuity Plan (BCP)

SessionCam has a business continuity plan which covers office locations and continuation of meeting contractual commitments. The plan is aligned with our information security framework, ISO 27001 and is reviewed on an annual basis.
SessionCam’s security culture is led by a Senior Information Security Manager with extensive industry experience. We recognize that security does not stand still and this makes us dedicated to continuously improving our security practices.

**Infrastructure**

- Access to customer data is restricted to the customer and the customer’s account team, who only access the account to provide support. All access is logged and monitored on a monthly basis.
- Similarly, access to SessionCam infrastructure is restricted to known, authorized IP addresses.
- Staff access to the corporate systems uses Two Factor Authentication (2FA) to log in.
- Both on-site computers and devices taken off-site are equipped with the latest version of industry-leading anti-virus and malware protection software. Any potential suspicious activity is logged and preventative action is taken if necessary.

**Human resources**

SessionCam staff are extensively vetted before they join the company. Standard checks undertaken include:

- Right to work in the UK
- Identity check
- Qualifications and five-year employment history
- Asking for, and contacting past employment (references)
- Basic DBS criminal record check (previously known as CRB)
- Credit and financial checks (including CCJs)

In the first week of employment, all staff take an information security awareness course which includes an introduction to the SessionCam security framework, data classification, the secure handling of sensitive data and understanding the risks an individual takes on. This course is retaken on an annual basis by all employees, including senior management and the CEO.

The contract of employment covers the expected behavior in dealing with sensitive information, security policies and procedures, as well as a non-disclosure agreement. Employees who fail to continually meet expected standards receive further training and are closely monitored until the required standard is consistently achieved.

**Our people**

- Staff are given photograph ID cards and a lanyard to confirm identity, while visitors to site are asked to sign-in and out using our visitor log.
- Access to our offices is security-controlled and we have CCTV throughout the premises.

Questions? Email support@sessioncam.com or contact your Account Manager for more information.
The easiest way to find your conversion problems

UK +44 (0)1603 618382
USA Toll Free – 1 888-528-0896 | Local – 1 619-382-2131
sessioncam.com

About SessionCam

SessionCam is a SaaS solution designed to help companies across the globe to optimize the online customer experience and find website conversion issues. We do this by taking an intelligence-based approach - using machine-learning algorithms to easily identify, visualize and understand your customers’ points of struggle and deliver prioritized, high-value recommendations.

Founded in 2009, we are one of the most experienced and mature solutions available, setting the global standard for measuring customer struggle.

facebook.com/sessioncam @sessioncam Linkedin.com/company/sessioncam-ltd