hotjar

Information Security Policy for Suppliers

Author:	James Moos - Security Team Lead
Date:	24th April 2023
Version:	v1.0
Approved By:	Ken Weary - Chief Operating Officer

Table of Contents

Introduction

1. Information security plays a crucial role in protecting Hotjar as a business, as well as interested parties that include (but is not limited to) customers and team members.
2. ‘Cyber attacks’ are commonplace and do not always begin as targeted attacks. Hotjar faces many different information security risks, which are constantly evolving.

Purpose

3. This policy sets out requirements for information security across Hotjar, with the aim of:
    a. Protecting customer and team data.
    b. Safeguarding Hotjar systems and reputation.
    c. Providing assurance to prospective customers in a transparent manner.
4. This policy forms part of Hotjar’s Information Security Management System (ISMS).

Scope

5. This policy applies to any suppliers or other relevant parties that may be granted access to Hotjar systems and/or data.
6. The security rules within apply to all of the following:
    a. All Hotjar data.
    b. Any Hotjar asset provided or to be used for Hotjar business purposes.

Security Objectives

7. Hotjar’s information security objectives are to:
    a. Ensure the confidentiality, integrity and availability of systems and data.

   b. Promote and maintain customer confidence and trust.
   c. Promote and maintain a secure working environment and behaviours.

8. Hotjar maintains an ISMS to provide a framework to these security objectives.

Responsibilities

9. It is everyone's responsibility to help build and maintain Hotjar's information security, including any Supplier we use.
10. The Supplier's leadership team is responsible for ensuring that any employee, contractor or other person engaged by the Supplier to provide services to Hotjar abides by this **Hotjar Information Security Policy for Suppliers** and the **Hotjar Acceptable Use Policy**.
11. The Hotjar Security Team is responsible for delivering and maintaining the ISMS and information security strategy and program.
12. The Security Team can be contacted at security-team@hotjar.com.

Security Incidents

13. Any potential or suspected security incident involving Hotjar assets must be reported **immediately.**
14. A security incident is any negative event that could potentially affect the confidentiality, integrity or availability of Hotjar assets.
15. A Hotjar asset is any data, system or equipment that we own or use. Examples of each are:
    a. **Data** - Hotjar team member records, customer data, company documents.
    b. **System** - accounts and tools (software - whether cloud based or local).
    c. **Equipment** - company provided laptops.
16. Examples of a security incident include:

a. Compromise of a password.

b. Accidentally signing in using a suspicious website/link.

c. An email containing sensitive information that is sent to the wrong recipient.

d. Confidential customer information that is inadvertently exposed.

e. Customer end-user data has been leaked outside of approved Hotjar systems.

17. In the event that a security incident involves personal data, the Hotjar Security Team will involve Hotjar's Data Protection Officer (DPO).

Data Classification

18. Hotjar uses a data classification scheme to indicate the sensitivity of data.

19. This scheme should be followed at all times to protect information appropriately. Suppliers must ensure that any data stored or processed by them is treated with the correct protection.

20. Some default rules apply:

    a. Data access is on a need to know basis.

    b. All customer data is considered **RESTRICTED.**

    c. Only people with a legitimate business need may interact with **RESTRICTED** data.

Classification	**Overview**
PUBLIC	Information that can be shared or viewed with the public without any restriction.
INTERNAL	Non-public information that is intended to only be shared or viewed internally by Hotjar team members. This information may be made available to third parties if a Non-Disclosure Agreement (NDA) is signed.
RESTRICTED	Information that is only available to Hotjar team members who have a legitimate business process on a need to know basis. This information

	should not be disclosed to third parties under any circumstances except to meet legal obligations and with approval from a Hotjar Senior Exec Leader.

Password Requirements

21. It is imperative that everyone adheres to the secure design and maintenance of passwords. Passwordless access is also permitted where the authentication method is of an equivalent nature.
22. You must meet the following password requirements where passwordless access is not in use:
    a. Minimum of 12 characters in length.
    b. Use a different password for every system/account.
    c. Never reuse old passwords.
    d. Change temporary or default passwords as soon as possible.
    e. Passwords must be stored in a secure password manager tool.
23. Individual account credentials must not be shared under any circumstances.
24. Where shared accounts exist, credentials must only be stored and shared using a secure password manager.
25. Any other types of credential, such as secret keys, must be securely stored and encrypted.
26. Secrets should only be shared where absolutely necessary for business reasons, limited to the smallest audience possible, and only distributed using a secure password manager.
27. If there is any suspicion that a password or other secret may have been compromised or known to anyone else, you must change it immediately and report a security incident.

Multi-Factor Authentication (MFA)

28. MFA, also commonly referred to as 2 Factor Authentication (2FA) is an important additional layer of security.
29. Wherever possible, MFA must be enabled by the account user.
30. Where physical security keys are used as a second factor, they must be kept physically secure and never left unattended.

Acceptable Use

31. Hotjar systems, data and equipment are all subject to the **Hotjar Acceptable Use Policy**. All users must read and adhere to this policy at all times.

Access Control

32. Access to Hotjar systems and data must only be provided where necessary to fulfill the duties of a specific role (role-based access control).
33. The principle of least privilege should be followed at all times to avoid granting excessive permissions.
34. Individual access should always be granted where possible, instead of shared accounts.
35. Hotjar's **password requirements** must be followed at all times.
36. Access should be reviewed whenever a user changes their role internally, and access changed/revoked as appropriate.
37. Access must be removed without delay when a user leaves Hotjar or no longer requires said access. The Supplier must inform Hotjar in the event of a departure to ensure any accounts are removed without delay.

Removable Media

38. As per the **Hotjar Acceptable Use Policy**, removable media such as USB sticks and external hard drives are not permitted by default due to the risk of data loss and malware.
    a. Specific exceptions may be requested by contacting the Hotjar Security Team where there is a business need.
    b. Where an exception is approved, the following requirements must be met:
        i. Any approved removable media must only be used for business purposes and not connected to any other device except for Hotjar computers.
        ii. Any Restricted data must be protected by encryption.

Physical Security

39. The Supplier must maintain a good level of physical security at any premises where services to Hotjar are provided from.
40. Everyone has individual responsibility to ensure that their local environment is physically safe and secure.
41. Any computing devices accessing Hotjar systems or data must have the screen locked when unattended.
42. Any computing devices accessing Hotjar systems or data must be kept secure at all times and never left unattended.
43. Printing Restricted or Internal information should be avoided unless absolutely necessary - to help the environment and avoid security risks.

Third Party Vendor Management

44. Systems and tools provided by third party vendors must not be used until they are approved by Hotjar.
45. Requests should be made using Hotjar’s procurement process to request a new system or tool.
46. The Hotjar Security Team will carry out a security assessment of the third party vendor prior to granting approval.
47. No access to company data or systems is permitted until an individual has commenced employment or has a suitable confidentiality agreement in place with Hotjar.

Device Security

48. Smartphones and tablets owned or used by Suppliers or their staff are only permitted to access Hotjar systems provided they meet/exceed the computing devices requirements below..
49. Hotjar-issued or Supplier-issued computers are to be used for work purposes. Only when these are not provided, the use of personal computers may be used but only provided they meet/exceed the following requirements below.
50. Supplier computing devices accessing Hotjar assets must meet the following requirements:
    a. The device is password or biometric protected.
    b. The device is fully encrypted.
    c. The firewall is turned on.
    d. The operating system and applications are kept up to date.
    e. The device has antivirus software installed and receives regular updates.

Secure Disposal and Reuse

51. Supplier computers must be securely erased prior to either disposal or reuse.
52. Any paper-based notes or printouts should be destroyed (e.g. shredded) prior to disposal if they may contain Hotjar Restricted or Internal information.

Email and Cloud Sharing

53. Email messages, and particularly any links or attachments, should not be opened if they are not from a trusted source or an expected message.
54. Cloud-hosted documents and files must only be shared with explicit recipients where necessary.
55. Particular care should be taken when sharing documents and files to external recipients.
56. Public sharing links (where anyone with the link may access the file or document) must not be used unless the classification of the contents is Public.

Remote Working

70. Always remain vigilant when working in a public space. Be aware of risks such as:
    a. Unauthorised people observing your screen
    b. Unauthorised people accessing or modifying the computer, including inserting USB devices.
71. Avoid conducting sensitive business matters in public.
72. Any confidential work should only be conducted from a private space.

Document History

Document History		
Date	**Version**	**Summary of Changes**
18/04/2023	v0.1	First draft of document created.
24/04/2023	v1.0	Final amendments and submission for approval.
