hotjar

Acceptable Use Policy for Suppliers

Author:	James Moos - Security Team Lead
Date:	2nd May 2023
Version:	v1.0
Approved By:	Ken Weary - Chief Operating Officer

Table of Contents

Introduction

1. Hotjar provides a range of different assets to be used in the course of business. It’s extremely important to use them in the correct way to act responsibly in line with our company values, and in a manner that is appropriate and legal.
2. An asset is any item that can be considered valuable to (but not necessarily owned by) Hotjar. Examples of assets include:
    a. IT assets - such as computers.
    b. Software assets - such as Google Mail or Slack.

Purpose

3. The objective of this policy is to provide clear rules about how to use Hotjar IT equipment, systems/accounts and data.
4. This policy also explicitly identifies certain behaviours or activities that are not permitted.
5. It forms part of Hotjar’s Information Security Management System (ISMS).

Scope

6. This policy applies to any person providing services to Hotjar on behalf of a Supplier, with access to Hotjar IT equipment, systems/accounts or data.

Responsibilities

7. Members of the Supplier’s leadership team are directly responsible for enforcing the policy and standards within their team and for adherence by their team.
8. All users have a responsibility to adhere to the policy and standards regardless of their status.
9. Hotjar's Security Team is responsible for maintaining this policy and providing advice on implementation.

Security Incidents

10. Any potential or suspected security incident must be reported **immediately** to security-team@hotjar.com.
11. A security incident is any negative event that could affect the confidentiality, integrity or availability of Hotjar assets.
12. 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.
13. 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 Hotjar systems.
14. In the event that a security incident involves personal data, the Security Team will involve Hotjar's Data Protection Officer (DPO).

General Use and Ownership

15. Any IT equipment, applications, accounts, data and other asset types provided by Hotjar remain the sole property of Hotjar.
16. These assets are provided to users so they can carry out their professional duties. Users are expected to take due care of these assets. Personal use is not permitted.
17. All software licences and tools must be used in accordance with any associated licensing rules from vendors.

18. Users must take due care to protect and maintain any equipment or asset assigned to them.

19. Users must return any assets to Hotjar when requested, as well as upon the termination of the contractual relationship.

20. Hotjar may access, monitor, inspect, search or record information or activities on Hotjar assets (such as computers, accounts, email and data) without limitation or notice.

21. Hotjar commits to only exercising the above right where absolutely necessary and in a manner proportionate to the requirements.

22. All use of Hotjar assets must be in compliance with all other company policies in addition to this Acceptable Use Policy.

Unacceptable use

23. The following are deemed as unacceptable use, regardless of whether it is for business or personal reasons:

    a. Any activity that may adversely impact or damage the reputation of Hotjar.

    b. Sending unsolicited emails such as spam or chain-mail messages.

    c. Sending emails with contents or attachments that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive.

    d. Use of material that infringes any copyright, trademark, patent, trade secret or other proprietary rights of a third party. This includes unauthorised copying of copyright material, digitization, and distribution of copyright photographs, software.

    e. Downloading and use of any unlicensed or ‘hacked’ illegal software.

    f. Material likely to encourage an illegal act.

    g. Information about, or software designed for, breaching security controls or creating computer viruses.

    h. Material that is obscene, sexually explicit, defamatory, incites or depicts violence, or describes techniques for criminal or terrorist acts (unless it is related to a customer support issue).

i. Material that is illegal under local or international law.

j. Material that conflicts with Hotjar's Core Values.

k. Compromising security controls of Hotjar, its customers, or any other person or organisation.

l. Any activities that intentionally adversely affect the ability of others to use Hotjar services.

m. Making any statement on your own behalf or on behalf of Hotjar that may cause offence, libel or damage the reputation of others.

n. Forwarding business data or emails to personal email accounts.

24. If in doubt about whether or not an activity is considered unacceptable then do not do it. If you require advice then please contact the Hotjar Security Team (security-team@hotjar.com).

Acceptable Use of Hotjar Systems and Data

25. Accounts must be secured in accordance with password and Multi-Factor Authentication (MFA) requirements established in the **Hotjar Information Security Policy for Suppliers**.

Protection of customer information

26. Customer personal data must be protected from unauthorised access, modification or deletion as per the EU General Data Protection Regulation (GDPR).

Storing Hotjar work/data

27. Users should ensure they save any work or data on behalf of Hotjar in a location where it is suitably protected from accidental loss in the event of equipment failure.

28. Where appropriate, users must ensure all important data is saved onto Hotjar’s cloud storage tool.

29. Removable media such as USB memory sticks or external hard drives are not permitted, even for backup purposes, without the explicit permission of the Security Team. For more details, please refer to the **Hotjar Information Security Policy for Suppliers**.

Google Single Sign On (SSO)

30. This section only applies to Suppliers who are provided Hotjar Google accounts.

31. Where available, Hotjar permits and encourages the option to log in to approved tools or services via Google SSO for individual accounts.

32. Users must not:

    a. Log in to another individual's account, using Google SSO.

    b. Log in to shared accounts or services, using Google SSO.

Document History

Document History		
Date	**Version**	**Summary of Changes**
24/04/2023	v0.1	Adaptation from Hotjar’s Acceptable Use Policy to create a version suitable for Suppliers.
24/04/2023	v0.2	Various amendments.
02/05/2023	v1.0	Updates made as part of the approval process.