Introduction

HappyFox takes the security and data privacy very seriously. HappyFox runs a robust security and privacy program for data submitted by customers to our Services (“Customer Data”). This document describes measures taken by HappyFox to protect the security and data privacy of Customer Data.

Data Center Security

HappyFox is hosted on Amazon Web Services (AWS), which maintains multiple certifications for its data centers, including ISO 27001 compliance, PCI Certification, and SOC reports. For more information about their certification and compliance, please visit the AWS Security website and the AWS Compliance website.

Infrastructure Security

HappyFox infrastructure is hosted in a secure private network provided by AWS. Firewall rules are in place to restrict access to only necessary systems. We perform automated vulnerability scans on our production hosts and run intrusion detection and other security monitoring tools to detect suspicious activity on our systems. We also maintain detailed audit logs on any activity performed on the server.

Compliance

HappyFox is SOC2 Compliant. HappyFox has undergone a SOC 2 Type II Audit.

Architecture and Data Segregation

HappyFox is operated in a multitenant architecture that is designed to segregate and restrict Customer Data access across different Customers. The architecture provides an effective logical data separation for different customers via an unique Company ID. Further segregation is done by maintaining customer specific users which cannot access data for any other customer. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

Incident Management and Response

HappyFox maintains an incident management process for security events that may affect the confidentiality, integrity, or availability of our systems or data. Incidents are tracked in a ticketing system where incident response and communication are tracked.

Personnel Practices

HappyFox conducts reference / background checks on all employees before employment, and employees receive security training during onboarding as well as on an ongoing basis. All employees are required to read and sign our comprehensive information security policy covering the security, availability, and confidentiality of the HappyFox services.

Confidentiality

We place strict controls over our employees' access to customer data. The operation of HappyFox requires that some employees have access to Customer Data such as Operations and Customer Support to diagnose issues.These employees are prohibited from accessing Customer Data unless it is necessary to do so. Employees only have access to the data that they strictly need and it is provided on the basis of role and designation.

Logical Access Control

Access to production systems is provided to authorized members of the Operations team and the employees are required to connect to our VPN with Multi-factor authentication in order to connect to the servers. All activity in the servers are logged and audited periodically. Access keys and passwords to the systems are also rotated periodically for each user. A list of users with access to production systems are also periodically audited.

Encryption in transit and at rest

All data transmitted to HappyFox servers over the internet are encrypted over 256-bit SSL.

HappyFox stores backups in a highly durable and geographically redundant storage system and all backups are encrypted at rest. HappyFox offers encryption at rest for Customer data on Enterprise plan on request.

Disaster Recovery

Customer Data is stored in a highly available redundant location managed by our hosting provider. We have well-tested backup and restoration procedures, which allow recovery from a major disaster. We also test our Disaster Recovery plans periodically to ensure that our procedures are up to date. Customer Data is automatically backed up nightly and is periodically tested.

Viruses

HappyFox does not scan for viruses that could be included in attachments or other Customer Data uploaded into the Service by a customer. Uploaded attachments, however, are not opened or executed by us and therefore will not damage or compromise our servers by virtue of containing a virus.

Product Security Features

- Authentication options - For admins/staff members we support HappyFox sign-in, SAML, and Google Apps Authentication. For end-users we support HappyFox sign-in, SAML, JWT and social media SSO (Facebook, Twitter, Google).
- Configurable Password Policy - HappyFox allows admins to set a password policy for all staff members. This feature is available on the Enterprise plan
- Role based Access Control - HappyFox allows users to define custom roles based on granular ticket level and managerial permissions and associate them to individual staff accounts. Access to tickets can also be restricted on the basis of Categories in HappyFox.
- IP restrictions - Access to the staff portal can be restricted by whitelisting specific IP addresses