happyfox

Data Security

Overview

HappyFox is committed to provide robust security for all its customers and their data stored across all its products & services. We consider Security our top priority while building & operating our enterprise grade customer support platform. Hence our controls span across hiring practices, software architecture, data center and other operations across the organization.

We serve over 12,000 companies in 70+ countries across multiple verticals such as education, media, e-Commerce, retail, information technology, manufacturing, non-profit, government and many others that have internal and external support functions.

This document provides an introduction to HappyFox's approach to managing security throughout its platform.

Table of Contents

Cloud Infrastructure Physical Security

HappyFox leverages all these controls in hosting its applications and customer data in AWS data centers. Our platform is primarily hosted on their Data centers in the United States and European Union.

AWS Data Center Security Controls Include

- High availability and redundancy built into all of its site design and operations.
- Physical access controls including employee access policies, regular access reviews, access logs, 24/7 monitoring and CCTV surveillance.
- Secure asset management and media destruction policies.
- Facilities such as Backup power, HVAC systems, fire suppression equipment and other controls to protect servers from environmental risks.
- Business continuity plans and Disaster recovery testing done to provide quick resolution & turn around time during disruptions of any kind.
- Regular third party security attestations for all the security and compliance controls built into their data centers and services. HappyFox reviews these attestations regularly to fulfill its security and compliance requirements.

Cloud Infrastructure Physical Security

Our engineering team drew on its experience of building & operating cloud services when choosing Amazon Web Services (AWS) as our Cloud Infrastructure partner. AWS is an ISO 27001, PCI DSS Service Provider Level 1 and SOC 2 compliant provider

Learn more about AWS Data Center Controls here

https://aws.amazon.com/trust-center/data-center/our-controls/

- **CCPA/CPRA:** HappyFox is CCPA/CPRA compliant. Please refer to our Privacy policy for CCPA/CPRA related information.
- **HIPAA :** HappyFox is HIPAA compliant.

Secure Personnel

Dedicated Security team, reporting directly to CEO, oversees all aspects of security in organization, Cloud Infrastructure and Product security. Our high level of focus on security starts with hiring, training and other operations inside the organization.

- **Background Checks:** All employees go through relevant background checks and reference checks before they get hired.

- **NDA/Confidentiality:** All new hires are required to sign Non-Disclosure and Confidentiality agreements and give acknowledgements on internal information security policy.

- **Software Access:** All software access is provided based on the Principle of Least Privilege (POLP) such that employees only have enough access to perform the required job. All access is removed once they leave the organization. Regular reviews are conducted while they are with the organization to maintain access only to relevant data. Access management is entirely carried out using an internal ticketing system.

- **Security Training:** Regular security training is conducted across all departments and organization units to give awareness about different forms of social engineering, phishing and other possible attacks, and give tools/best practices in avoiding them.

Secure Software Development Life Cycle

HappyFox adopts Secure Software Development Framework when building its applications and services. Our tools, frameworks and processes follow latest Industry standards and conventions to mitigate security risks early in the development phase.

- **Secure Frameworks:** Libraries and frameworks used to build our products have in-built mitigations for common OWASP vulnerabilities such as SQLi, XSS (Cross site scripting), CSRF (Cross site request forgery), etc.

- **Isolated Development & Staging Environments:** Our development and staging environments are fully isolated from production environments. We do not use any form of production data in these environments.

- **Peer Reviews:** All changes to application code go through peer reviews before they get approved for release to customers.

- **Quality Assurance:** All changes made to the application go through a strict quality assurance process to find & resolve correctness & security issues on business logic, before they get released to customers.

Secure Software Development Life Cycle

- **Static Code Analysis:** Source code is scanned by static code analysis tools periodically for detecting common security issues such as SQLi, IDOR, etc.
- **Dependency Vulnerabilities:** We use third party tools to identity and resolve vulnerabilities on the third party libraries used to build our applications.
- **Penetration Tests:** Trained and experienced in-house security testing team does penetration tests using modern DAST (Dynamic application security testing) tools on all modules to identify and report on OWASP vulnerabilities.

Secure Customer Data

Cloud security for our applications hosted in AWS is top priority. HappyFox platform takes full advantage of the hosting environment and services provided by AWS to secure customer data across compute, network and storage layers.

- **Compute Security:** HappyFox applications are hosted on secure isolated VMs provided by AWS Elastic Compute Cloud service (EC2) and related services. AWS ensures that no two VMs share common memory space. VMs are fully scrubbed when they are deleted.

- **Network Security:** All VMs are hosted inside isolated AWS Virtual Private Cloud (VPC). Sensitive VMs are hosted in private networks within the VPC to ensure that no one can access them directly.

- **Strong Firewall:** VMs use specific firewall rules to guarantee they open up only the ports required for applications and services to function and only to specific servers that need them.

- **Encryption in Transit:** Data transmission from users to HappyFox via our Application UI or API happens via encrypted HTTPS/TLS connection (using at least TLS 1.2 protocol, RSA and 2048 bit keys) at all times. This is to ensure data gets securely transferred to HappyFox when users are using our applications in public untrusted wifi spots or in private wifi spots such as Home/Office network.

Secure Customer Data

- **Encryption at Rest:** All data is stored in encrypted volumes, by using one of the strongest block ciphers available to encrypt your data, 256-bit Advanced Encryption Standard (AES-256).
- **Secure Backups:** HappyFox takes regular backups, encrypts them using AES 256 bit standard and stores them off site. Backups are internally stored in at least two AZs for additional redundancy.
- **24/7 Intrusion Detection:** All servers and VMs are monitored 24/7 by advanced IDS and anti-malware tools to raise alerts when any anomalous activity is detected.
- **Vulnerability Scans:** Regular vulnerability scans are performed in the servers to identify & fix vulnerabilities.
- **Multi A-Z Deployment:** VMs are hosted in multiple availability zones within a VPC to ensure application and data availability even in times of network failures.
- **Restricted Access:** Access to the production environment is restricted to few trained & authorized personnel in the organization. Strong multi-factor authentication and encrypted VPN connections are enforced in all such access. All of this is audited and monitored regularly by the operations team.

Product Security

HappyFox enables customers to protect their account and its data by providing Enterprise grade security settings and capabilities.

- **Multiple Authentication Options:** Agents can login via password based authentication or SSO (Single Sign On) via Google Apps or Enterprise SSO via SAML. End users can login using social media SSO logins (Twitter / Facebook) or Google apps SSO or password based authentication.

- **2-FA:** Two factor authentication is available for agents via an Authenticator app.

- **Customizable Password Policy:** Customers can set up their own password policy to enforce strong passwords, periodic password rotation & expiry to fulfill their own security requirements and access policies.

- **Proactive Alerts:** Email alerts are sent to agents when there is a failed login attempt or when there is a password reset attempt on their account.

- **Account Lockout:** Agent logins are locked when login attempts fail for a certain number of times beyond a threshold. This is to ensure that brute force attack based on password is mitigated.

Product Security

- **Encrypted Passwords:** Passwords are encrypted and stored by strong oneway hashing techniques to fully eliminate possibilities of reading/decrypting them.
- **Automatic Logouts:** Customers can configure to logout agents automatically after a period of inactivity.
- **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 agent login can be restricted by whitelisting specific IP addresses.

Note: Product security features availability depends on product and plan chosen.

Security & Penetration Tests

As part of its security strategy, HappyFox carries out following security and penetration testing activities.

- **In-house Penetration Tests:** As a continuous effort, our security testing team does penetration tests on all our products against OWASP and other latest security threats. Testing team uses more modern tools to identify and report on such issues.

- **Bug Bounty Program:** HappyFox runs an active private bug bounty program in partnership with HackerOne to invite third party security researchers to perform penetration tests on our products. Security researchers get this avenue to find vulnerabilities and report them safely to us. This in turn enables our team to fix them sooner and strengthen security on our platform.

Business Continuity and Disaster Recovery

As part of its continuous effort to improve reliability and resilience of our platform, HappyFox has clear business continuity and disaster recovery plans and procedures.

- **Business Continuity Plan:** HappyFox has a documented business continuity plan that outlines measures to avoid and lessen impact of unexpected disruptions in our business operations. It includes operational details about steps to take before, during, and after an event.

- **Disaster Recovery Procedures:** HappyFox has outlined clear recovery procedures and metrics in cloud infrastructure and operations to lessen the impact of different unexpected disruptions in our platform.

- **Testing and Improvement:** HappyFox business continuity plan and disaster recovery procedures are supported by regular testing that includes simulations of different scenarios. During and after testing, HappyFox documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

- **RTO:** 24 hrs

- **RPO:** 24 hrs

Availability and Performance Monitoring

To ensure that our web services are running as expected for customers, we have implemented 24/7 monitoring to gain complete visibility over Applications, System Infrastructure, Network and other supporting services.

- We also monitor performance of all APIs and applications including average response time, average throughput to identify bottlenecks and continuously improve our design and scale our capacity to meet the growing demand.

- We also monitor performance of all APIs and applications including average response time, average throughput to identify bottlenecks and continuously improve our design and scale our capacity to meet the growing demand.

Incident Response and Management

To have an organized response to incidents, isolate & resolve them quickly while keeping customers and other stakeholders in loop, HappyFox has established policies and procedures in place that get implemented in the following ways.

- HappyFox has a dedicated team on call to respond to all incidents.
- We maintain a comprehensive incident response plan which outlines the procedures we follow during and after an incident.
- Incidents are tracked in a ticketing system according to the documented plan, where incident response, communication, root cause and post mortems are tracked.

Compliance and Certifications

SOC 2 Type II
Compliant

GDPR
Compliant

HIPAA
Compliant

CCPA
Compliant

CPRA
Compliant

By adopting Industry accepted security & privacy frameworks and continuously demonstrating them year after year, we have achieved following certifications and compliances across all our products and services. This ensures that we have best security controls implemented towards safeguarding our customer accounts & data and in turn enable them to meet their own security and compliance requirements.

- **SOC 2 Type II Certified:** As part of its commitment to security, HappyFox has used the AICPA SOC 2 Type II process to successfully design and build the operational and security processes of its products and the organization. Customers can access the latest third party SOC2 audit report on signing our NDA. Please write to support@happyfox.com to request the report.

- **GDPR:** HappyFox is GDPR compliant and it enables its customer to be GDPR compliant as a data processor. Please refer to our Privacy policy & GDPR documentation for more details

- **CCPA/CPRA:** HappyFox is CCPA/CPRA compliant. Please refer to our Privacy policy for CCPA/CPRA related information.

- **HIPAA :** HappyFox is HIPAA compliant.

Thank You

happyfox.com/data-security