TravelPerk Security Whitepaper

TravelPerk

Table of Contents

Introduction

Information security has never been more relevant than now. We see news reports almost daily of cyber attacks on businesses - affecting confidentiality, integrity or availability.

Nevertheless, many businesses understand the benefit of adopting Software-as-a-Service (SaaS) technologies. By carefully selecting trusted providers, your business can leverage incredible technologies with greater features, scalability and pricing than on-premise solutions could ever offer.

For us, we believe that our very success as your trusted business travel partner can only exist through robust security and data protection measures. We store and process personal information such as passport details, travel itineraries, and more. This is why we aren't settling for the security measures we describe to you in this whitepaper but instead are focused on continual improvements.

We're sharing this whitepaper to return the trust you've placed in us, providing a level of transparency that we hope provides you with assurance and confidence in our partnership. It outlines our approach to security, data protection and compliance for TravelPerk, and our business travel offering.

TravelPerk's security culture

Security starts and ends with people, and so we spend a great deal of time and money on keeping our team aware of security and data protection issues and risks. But we don't stop there.

Awareness simply isn't enough. What we focus on is modifying end-user behaviours. Our team are all owners in what they do, and so we take this company value a step further by empowering people to make the right decisions. We regularly present on security topics in our company 'all hands' weekly meetings.

Our dedicated security team

Naturally, none of the contents of this whitepaper would be possible without a team of security professionals who work hard to continually improve our security.

We have a team of specialists with extremely diverse backgrounds across a range of industries. Our expertise spans everything from information security, technical security, product security, digital forensics and vulnerability management.

They are responsible for acting as ambassadors when it comes to security and data protection matters across the company, frequently providing consultancy to other teams and departments. We actively scan for issues, vulnerabilities and suspicious activity.

We maximise the security talent available to us by also engaging with various external experts to support independent bug bounty program.

Our data protection team

At TravelPerk, we have a dedicated privacy team and an assigned Data Protection Officer (DPO) who work closely with our security team to ensure the protection of personal data entrusted to us.

The privacy team engages with you, our customers, to support any data protection queries or the exercise of data subject rights. They also work closely with other departments including product, engineering and customer care to ensure that we strive for continued excellence.

Information Security Management System

Our security program is operated as an Information Security Management System (ISMS), using ISO 27001 as a reference guide. We also use many 'Annex A' controls from the standard, alongside a large number of our controls.

We take a risk-based approach in all we do - helping to focus on having a greater impact. Our ISMS includes a variety of policies and procedures, with the main ones outlined below.

- Information Security Policy
- Data Protection Policy
- Acceptable Use Policy
- IT Administration Security Policy

Keeping current with the security industry

The global threat environment we work in is constantly changing, and we recognise the need for our teams to keep up to date, applying this knowledge to protect our customers.

We have a dedicated budget for specialist training and proactively encourage our team members to undergo training. We also have a variety of information feeds frequently coming in - including security news, vulnerability releases, and updates from data protection authorities such as the UK's Information Commissioner's Office.

We're also a corporate member of the Chartered Institute of Information Security (CIISec). We develop our team members using CIISec's industry-recognised skills framework, by attending events, and also look to contribute back to the security industry where possible. After all, information security is a team effort and collaboration is key!

HR Security & Awareness

Hiring Procedures

Security begins before the employee even joins us. It's well known by candidates that we have a fairly thorough hiring process, including an emphasis on hiring great cultural matches - which helps to identify individuals with the right values and ethics. Before they join us, our People team performs background reference checks to verify an individual's previous employment history and education.

Security training for all employees

All TravelPerk employees (and relevant contractors) undergo security and data protection awareness training as part of their onboarding in the first weeks of employment. This is led by our security team and designed based on the environment and threats that we face.

We also carry out annual awareness training for existing employees - this is specific to their role, which helps to keep the information we share relevant and engaging.

Additional awareness initiatives

We don't believe in a 'tick box' approach for awareness and culture, so we strive to go above and beyond to continually engage our team throughout the year - not just once a year for mandatory training.

We've run a variety of different initiatives and this list is constantly growing. We're using artificial intelligence to run simulated phishing campaigns, helping us to identify and support users most at risk - and educate them better. We've hosted internal 'Capture the Flag' (CTF) style events for engineers, and even competed against other businesses in a business-only CTF event.

We proudly display a variety of awareness posters around our offices internationally, designed in-house by our security team and graphic designer. We also have a gamification approach in TravelPerk security, secure behaviours are rewarded.

Operational security

As a technology-focused company that regularly releases new product features and is growing from success to success, we spend plenty of time working in security operations.

Secure user access provisioning and authentication

We use a company-wide identity and access management tool to centralise provisioning and decommissioning of user accounts in TravelPerk. This tool allows us to securely manage user identification and to apply security policies for accessing business applications.

Vulnerability management

Periodic penetration testing simply isn't enough for a fast-changing environment like ours. So we take our vulnerability management much further.

We conduct daily dynamic vulnerability scans of our web application, while our mobile application is also scanned daily with a variety of static, dynamic and interactive testing. We have implemented a fully managed bug bounty program, which gives us access to a large number of security researchers to help identify and report bugs or vulnerabilities to us before bad hackers do. This means that our critical platforms are being tested 24/7 and that the findings are reviewed and acted upon according to severity.

Malware prevention

As you might expect for an international company like us, we leverage world-class endpoint detection and response tooling. Using behavioural detection, we believe this helps to protect us from next-generation attacks that signature-based systems won't recognise. It also means we can quickly connect and respond to an endpoint incident anywhere in the world.

We also have various solutions in place to ensure malicious software doesn't enter our systems or travel applications.

Monitoring

We collect activity and access logs and important information from a variety of different sources. Where we receive any alerts or other triggers, our team inspects and investigates using a variety of tooling. Wherever possible, our tools are configured to detect suspicious activity and bring it to our attention without delay.

This includes monitoring and alerts from across our own IT estate and tooling, in addition to our business travel applications.

Incident management

Our security team is trained in taking the lead for any security incident that might occur - getting the right people into the room and coordinating any response required by following our Incident Response Plan. We don't introduce bias early on by assuming a severity level from what might initially be limited information - instead, we treat every incident with equally high priority and importance until we have information to prove otherwise.

We have an engineering on-call system 24/7 and and incident management team so that should an incident occur out of hours that affects confidentiality, integrity or availability, our engineers can respond, escalate and swiftly resolve any issue, supported by our security team.

We follow best practices by maintaining an incident tracker and analysing incidents afterwards to ensure lessons are learned, and any possible improvements are made.

Backup and recovery

We have a business continuity and disaster recovery plan to resort to for the most common scenarios and, we have several solutions in place to ensure the continuity of key business operations in the event of a disaster or outage.

Our cloud-based platform is hosted by Amazon Web Services, which has a number of solutions in place to ensure continuity, including equipment maintenance scheduling, environmental protections, as well as secondary and tertiary fallback sites on standby. All data is backed up daily within the environment.

The recovery time objective and recovery point objective are respectively 30 minutes and 1 day. All our business continuity measures take our information security requirements into account and this will remain a requirement for us in the future.

Asset management

All information processing assets, both systems and hardware, are maintained in TravelPerk's asset registry and are managed in compliance with our Information Security and IT Administration policies.

Physical Security

Our physical offices are protected by 24/7 monitoring. Key card access is required to ensure only authorised employees or contractors can access our buildings and office areas. Our offices are equipped with a video surveillance system.

Access to our stock room and network equipment is restricted to authorised staff only in line with our access management policies.

We also operate a clean desk and clear screen policy.

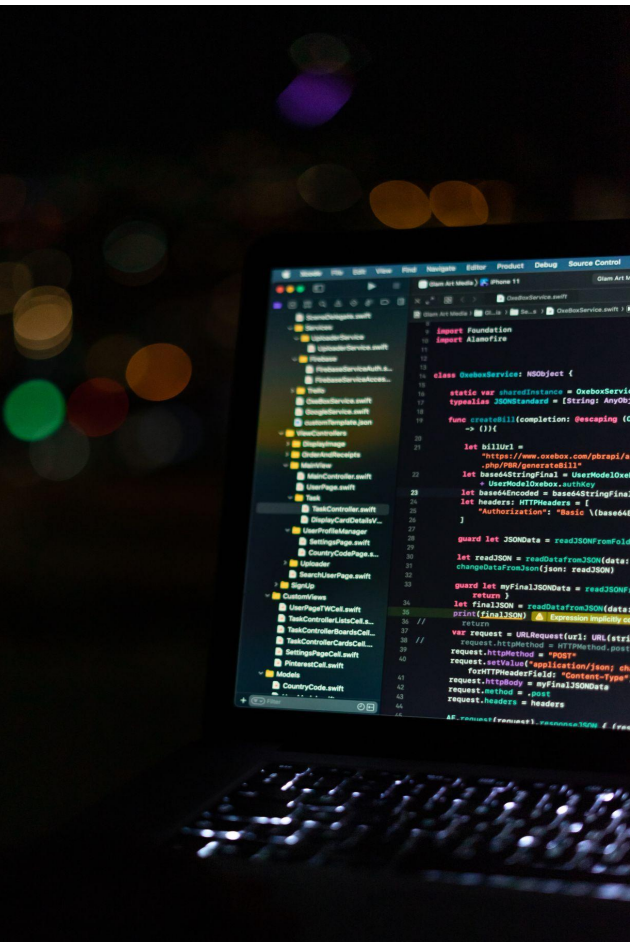
Our Product

Our business travel SaaS product is world-class, so we've ensured that it has top-class security measures to go with it.

High availability hosting

We host our production environment within Amazon Web Services (located in Ireland, EU). As you probably know, AWS comes with extremely high availability/uptime, and a range of security features and tools such as GuardDuty, TrustedAdvisor and Key Management System.

Amazon AWS means that our hosting environment is certified to a number of standards including ISO 27001 and SOC2.



Secure payments

Payment card information is another data type that is extremely important for us to protect alongside personal data. To do this, we've partnered with Stripe, since that's what they do best. This means that TravelPerk never stores or processes your payment card information - instead it's managed by Stripe, and we simply use unique reference numbers to connect with Stripe and charge you for bookings and services.

Secure releases

We update our code regularly, so follow best practices when it comes to pre-release checks. As well as code quality, we also run scripted checks that include security tests. Where code releases are identified by engineers as likely to affect security or data protection, our security engineers are called to review and approve the code.

Of course, there's no such thing as perfect code - and that's why we have daily vulnerability scans and a bug bounty program to have many layers of defence.

DevSecOps

We have a dedicated DevOps team a security champions program who own shared responsibility for securing our production environment. They continually monitor our compliance with the CIS Top 20 Benchmark for AWS and a variety of security tools, ensuring we comply with secure SDLC best practices.

Data encryption & password storage

Nowadays encryption is one of the most routine security controls anyone should expect when it comes to protecting confidential data.

We use AES-256 to encrypt your data at rest (including backups). For data in transit, we enforce a minimum of TLS v1.2 and don't support older legacy versions.

For password storage, we work according to NIST recommended standards with our choice of hashing algorithm and password stretching mechanism.

Our email system is also encrypted, automatically using S/MIME wherever supported.

Security features for you

Not all security has to be behind the scenes. There are several growing features that customers can benefit from when using our business travel applications.

Customers can integrate their existing identity providers via SAML/SSO, meaning you can also use your existing multi-factor authentication solutions.

To secure your accounts, we've set a password policy of 8 characters and also enforce account lockouts after a number of failed attempts. For customers who wish to use their existing Single Sign On (SSO) provider, you can also leverage your existing 2 Factor Authentication (2FA) as part of this setup.

We also imagine many customers want to restrict access to the information within your company account, which is why we offer a variety of different roles with limited-scope access

(premium/pro tier feature). It's down to you to decide who needs access to your information. From the central portal, customer administrators can easily provide or remove access.

7-star support

We've always believed that a core part of our offering is our amazing 7-star customer service, which is highly rated with amazing response times.

To maintain the 7-star theme beyond the user experience, we've also trained our customer care agents on how to deal with a range of possible security and data protection issues when handling tickets via calls, chats, and emails. We have documented procedures on how to check the identity and authorisation of the person contacting us, as well as a dedicated quality team who audit and carry out follow up training where necessary.

Service availability

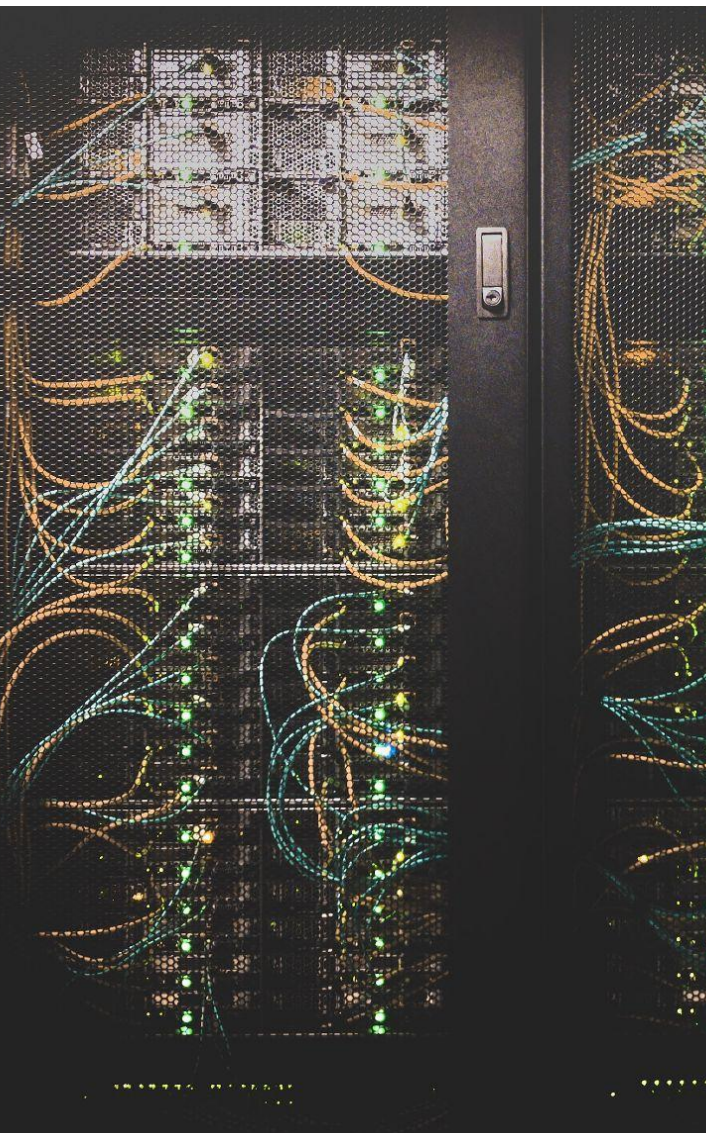
We understand that you want to ensure your travel information is readily accessible to you whenever your travelers need it.

Our Amazon AWS high availability hosting ensures maximum uptime, while our careful control of code releases alongside 24/7 on-call engineers means that in the unlikely event of a bug being released, we can quickly roll back in a matter of minutes (usually just seconds!).

Our customer care team are distributed in different countries and are kitted out to work remotely, meaning that should any service outage or environmental issue affect one of our offices, we can maintain a good level of service to support your travelers at all times.

Data access and restrictions

Your data is the most precious item we look after, and so we only provide access to it where absolutely necessary.



Internal restricted access

We have implemented role-based access control - so only certain people can access customer information where necessary to carry out their duties (such as customer care, or account managers).

We periodically check these accesses and continually verify whether our existing policies, procedures and tooling are fit for purpose, making improvements where necessary.

For customer administrators

Even for your trusted employees who you sign up as administrators in your TravelPerk account, certain information simply isn't revealed - all in the interest of security on a 'need to know' basis.

Administrators are able to update information such as ID numbers in their travelers' profiles, but cannot see the existing data, upholding privacy for each and every individual in your account.

Third-party suppliers

Naturally, to build such an incredible business travel platform, we've partnered with some other great organisations. In these scenarios, the security and data protection teams are involved to plan and help implement secure partnerships. In all cases, we carry out an initial audit and subsequent periodic audits to ensure security measures are being maintained to a high standard. We're also extremely transparent with all our customers about where any personal data is shared, as you'll find out below.

Protecting personal data

At TravelPerk, we recognise the position of responsibility we hold for our customer data. Our employees and contractors are trained about protecting personal data as soon as they join our team. We often observe topics being raised proactively by our wider teams when designing or selecting business solutions - a sign of both understanding and the importance that we place on protecting customer data.

Our commitment to you

As your trusted partner for business travel, we ensure that we uphold data protection requirements to the highest standards. Our data protection team provides clear information to fulfil the EU General Data Protection Regulation (GDPR) principles of:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

On our website, we've laid out an overview of data protection at TravelPerk and our privacy policy to provide you with information about how we meet all these principles. You'll also find our standard data processing agreement that governs our partnership with you, as well as security measures.

Data subject rights

Our team is prepared and ready to support you with carrying out any exercise of data subject rights by your team. We have internally built tools that allow us to support you as the data controller in fulfilling your obligations. You can also exercise your data subject rights by contacting our data protection team directly at **personaldata[at]travelperk.com**.

Data sub-processors

While we work hard to limit any onward transmission of customer data, there are certain circumstances where this is required - usually to provide an even better product to you. Nevertheless, we keep this list of data sub-processors as short as possible.

We send you data protection updates from time to time, including when we appoint new data sub-processors. We carefully maintain an up to date list of data sub-processors, clearly showing the purpose, location and mechanism for transfer.

You'll be able to find our latest sub-processor list on our website.

Conclusion

The security of your data is of paramount importance for us to operate effectively as your trusted business travel partner. We've gone to great lengths to secure your data through technical, procedural, personnel and physical measures, and we won't ever stop our efforts to continually improve.

We implement best practices across the business and empower our team with information and education so they can demonstrate positive security behaviours. Our investment into various security technologies means that we can keep a close eye on our security estate, as well as those of our third-parties, and quickly react to any issue that arises.

Thousands of customers around the world trust us to provide the best business travel experience possible, while also securing their data and acting as a trusted partner. We hope this whitepaper has given a useful insight into how we approach security at TravelPerk and as we grow further, we intend to continue expanding our security program with the same transparent approach.