Information Security

Section 1 – Overview of Information Security at Corporate Traveller

1.1 Goal

At Corporate Traveller our customers are our greatest priority and for this reason managing Cyber and Information Security risks is at the heart of everything we do. This document is intended to give an overview of our approach to information security to give confidence to our clients and travellers that their data is in safe hands. This statement is presented based on ISO/IEC 27001 which is the leading international standard for information security management systems (ISMS).

Worldwide, organisations implement and maintain an ISMS to protect data that is crucial to their businesses, mitigate risk and ensure stable operations, and to provide confidence to stakeholders and customers. The standard is grouped based on Control Sets, which are the topics contained within it. Corporate Traveller's approach to information security is aligned to this standard Corporate Traveller is committed to taking steps to ensure systems, in which their data is held, are appropriately and consistently protected against cyber and information security threats.

Section 2 – Control Set Statements

2.1 Information Security Policies

Flight Centre Travel Group, parent company to Corporate Traveller, has a set of security policies, standards and frameworks which flow down from an Information Security Statement which is signed by our most Senior Executive. This statement shows that Information Security has the support and backing of the most senior managers in our business, this support translates into an internal focus which ensures all staff work in a secure manner. Global Information Security and Privacy policies, standards and frameworks apply to all members of staff regardless of their job role. The policy set includes the expected policies e.g., Acceptable Use, Remote Working, Risk Assessment and Global Security and Privacy by Design Framework to name but a few. Where required there are local variations to these policies.

2.2 Organisation of Information Security

The Flight Centre Travel Group Board and Executive leaders of the organisation have assigned accountability for Information Security to our Group Chief Information Security Officer (CISO) to oversee Flight Centre's Information Security risk management practices, Strategy and Policy. The CISO is also supported by a global team to provide information security advice, guidance and support to all business areas, including the monitoring of Information Security risks, the threat landscape and that controls continue to operate effectively thus ensuring adequate maintenance of Security practices across the business.

The CISO regularly reports to the Executive Leadership team, Board and Risk and Audit Committee on matters regarding cyber and information security.

2.3 Human Resource Security

Corporate Traveller has on-boarding processes for verification of the identity of the potential employees, their right to work in the country, and verification of the prior employment through reference uptake, it also covers a criminal record check, where required based on role type and customer needs. Corporate Traveller also has policies on what must be done when an employee resigns or leaves the business, including risk assessments on when access should be removed.

Corporate Traveller has a centralised platform for delivering training to all employees, there are mandatory courses for any new employee to complete in their first couple of weeks, this includes several modules which cover their Information Security responsibilities, how to work securely, and on how to spot things like phishing and other internet-based threats. There are also requirements to repeat this training on an annual basis, plus augmented training if new threats arise that require communication to all employees. The training is updated annually to include the topical high risks facing organisations globally.

2.4 Asset Management

Corporate Traveller maintains an inventory of systems and platforms within which customer data is stored or processed, and processes that articulate how employees are expected to treat our data or data entrusted to us. We have asset repositories which detail who owns each item of data and other details relevant to that asset.

Corporate Traveller also has a protective marking policy which details how each classification is to be treated, and with whom each category can be shared.

Corporate Traveller also operates different controls for protection of data on mobile devices, including controls to prevent data based on higher classifications from leaving the organisation, and remote wipe capabilities should a device be reported lost or stolen. All portal devices that have access to Corporate Traveller data must be encrypted. Corporate Traveller utilises products such as Microsoft InTune, Airwatch, and Bitlocker to help achieve these control objectives.

2.5 Access Control

Corporate Traveller operates Role Based Access Control (RBAC) for our key systems and the access is audited. For lower risk systems it is a mix of RBAC and Access Control Lists (ACLs). This means that employees and customers only have access to systems and data for which they have a need. All Systems have an Asset Owner associated with them. Asset owners will determine the rules, rights and restrictions on user access to their assets based on the user requirements and associated security risks. The business requirements must be clearly stated in advance for the direct benefit of both users and service providers before access is granted. Other requirements are defined in the Access Control Policy.

Information Security

Corporate Traveller has strong controls around all external access to our systems which is supported by two factor authentication, this means that not only does a person have to have a valid logon and password, but also access to a secondary application which provides a onetime code to allow access to proceed.

2.6 Cryptography

Corporate Traveller encrypts all client data at rest and in transit in our systems and networks and has a policy for key management and storage. We regularly review our standards to ensure that our encryption keys and ciphers are maintained and updated with industry best practices, vulnerability disclosures and changes to our threat landscape.

2.7 Physical and Environmental Security

Corporate Traveller also have Physical and Environmental Policies to protect our assets both physical and logical. These details what controls are required to be implemented to adequately protect physical locations where our assets and data are held. This approach covers people, processes and technology to ensure appropriate security is maintained within key sites. Examples include a clear desk policy, the application of data disposal and handling practices, visitor policies, tailgating, etc.

2.8 Operations Security

Corporate Traveller has defined roles and responsibilities for the protection and maintenance of operational security controls including regular reviews to ensure that controls are designed and operating effectively. These processes and reviews are informed by threat intelligence with Corporate Traveller taking an approach of continuous improvement. Corporate Traveller monitor and mitigate risks associated with threats such as malware (i.e., Viruses and Ransomware) using technologies including end point detection and response, entity and user behaviour analytics and 24x7x365 SOC and threat hunting capabilities.

Corporate Traveller ensures suitable backup and disaster recovery processes are in place and regularly tested. Corporate Traveller has a robust approach to vulnerability management with the technology landscape regularly scanned and patches promptly applied based on risk. Corporate Traveller has a framework of Security and Privacy by design which informs the creation of new systems and processes within our business, development and testing of any software strictly follows this framework.

2.9 Communications Security

Corporate Traveller has policies which govern management of the security of networks, and requirements on perimeter controls which consider the risks of data traversing those links and perimeter locations. Our networks are extensive, and we have monitoring in place to ensure controls remain active and configured as required.

2.10 System Acquisition Development and Maintenance

Corporate Traveller has a Systems Acquisition Development and Maintenance Policy which alongside the Global Security and Privacy by Design Framework details how and when during the lifecycle of a development information security must be considered and put into practice. These first-line risk management processes are supported by second and third-line reviews including penetration tests as required. Static code analysis is conducted regularly using recognised and trusted products. Developers are subject to annual secure development training, using products such as Secure Code Warrior. The acquisition of any new system is subject to a security and privacy review conducted by the Corporate Security and Privacy team.

2.11 Supplier Relationships

Corporate Traveller operates under a Vendor Management Policy which details the processes required to be followed for each of our existing and new suppliers. This is based on a risk assessment for each supplier. All suppliers are required to answer an annual questionnaire as a minimum, but for higher risk suppliers, we meet them regularly but may also perform onsite audits for the highest risk.

2.12 Information Security Incident Management

Corporate Traveller has a robust Incident management capability, of which Information or Cyber incidents form a major part. We also undertake exercises to practice our response in this area. Corporate Traveller has a 24x7x365 Security Operations Centre and Threat Hunting capability monitoring our security health via our next generation Security Incident and Event Management (SIEM) platform, we have market leading incident response and forensic experts on retainer. Corporate Traveller has recently rolled out our endpoint detection and response capability across our business globally

2.13 Business Continuity Management

Corporate Traveller has defined and maintained continuity capabilities, which are also tested on a regular basis. Our robust business continuity plan forms part of our business standards. All third-party systems are also required to have their own BCP capability, as part of our supplier agreements.

2.14 Compliance

Within the department of the Group CISO there are assigned Compliance and Assurance roles across the globe, in regard to Information Security. The legal department, supported by our Independent Privacy team, are based in all geographies and are responsible for tracking and ensuring compliance with local legislative requirements.