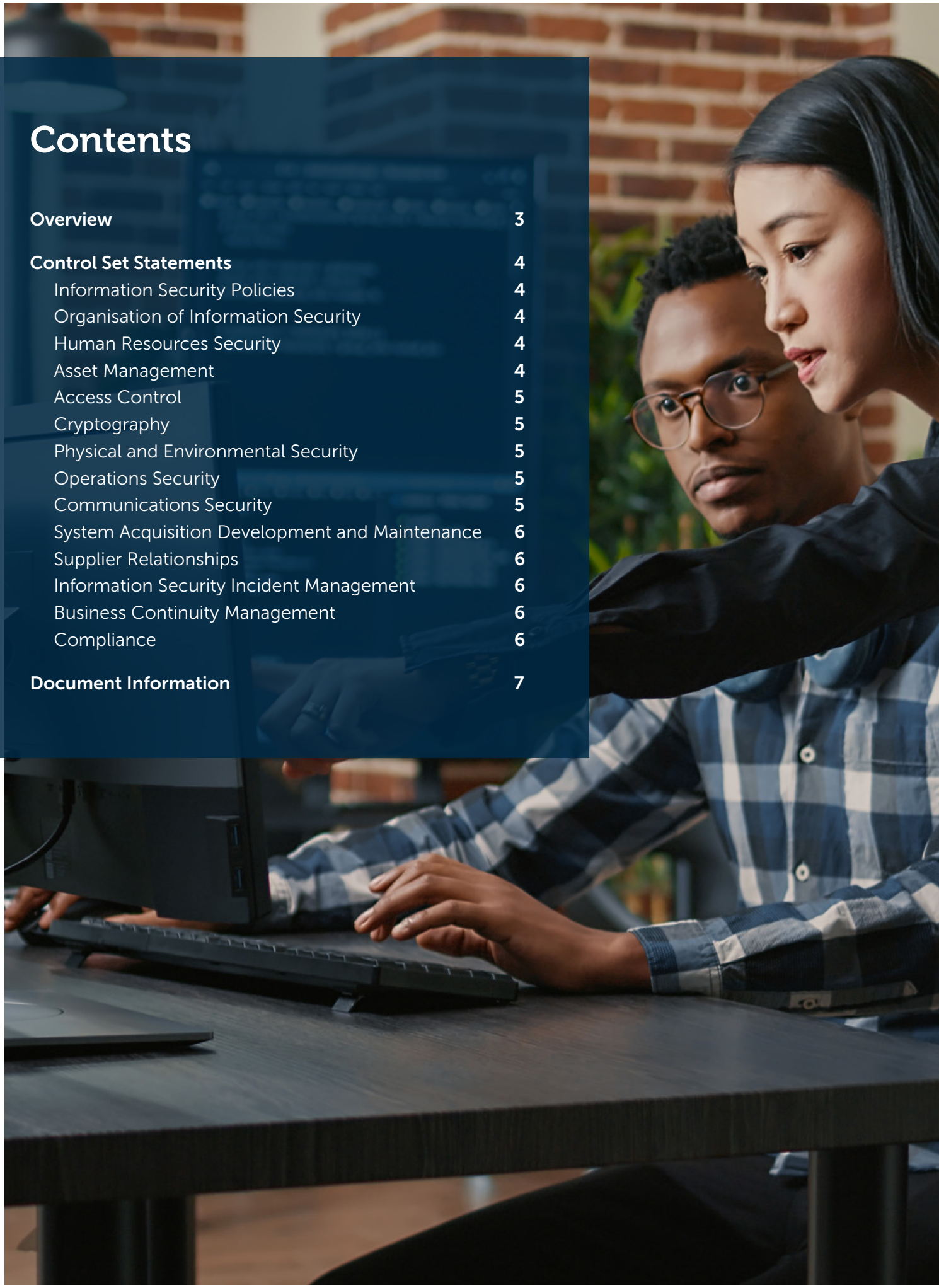
# Technical and Organisational Measures

# Contents





# Overview

At Corporate Traveller our customers are our greatest priority and for this reason managing Cyber and Information Security risks are at the heart of everything we do. Corporate Traveller is a wholly owned company of Flight Centre Travel Group (FCTG).

This document is intended to give an overview of our approach to information security to provide assurance to our clients and travellers that Corporate Traveller has taken appropriate steps to protect their data.

This statement is structured on ISO/IEC 27001 2013 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.

The Corporate Traveller security program is based upon ISO 27001. Whilst Corporate Traveller are not certified to the standard, Corporate Traveller Australia has started their journey and will be certified by the end of 2024, other Corporate Traveller regions will follow on from that certification in 2024 and 2025.

**Corporate Traveller are committed to taking appropriate steps to ensure the data and services entrusted to us by our customers are protected against cyber and information security threats.**

# Control Set Statements

## Information Security Policies

FCTG 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. There are 44 Global Information Security and Privacy policies standards and frameworks which apply to all members of staff regardless of their job role, plus a further 44 which cover HR and Information Technology Specific topics. Where required there are local variations to these policies.

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 4. Where required there are local variations to these policies.

## Organisation of Information Security

The Flight Centre Travel Group Board and Executive leaders of the organisation have assigned accountability for Information Security and Risk to our Group Chief Security Officer (GCSO) to oversee Flight Centre's Information Security risk management practices, Strategy and Policy. The GCSO has responsibility across Information Security, Enterprise risk and Privacy with the Global CISO, The GM Enterprise Risk and the Group Chief Privacy Officer part of the GCSO leadership team.

The GCISO 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 GCSO, GCPO and GCISO regularly report to the Executive Leadership team, Board and Risk and Audit Committee on matters regarding cyber and information security.

## Human Resources Security

Corporate Traveller has differing processes on-boarding individuals across the globe, but where possible (i.e. within local legislation) this meets the principles of the Baseline Personnel Security Standard (BPSS) created by the UK government to define the minimum requirements to be checked before an employee is on boarded. This includes verification of the identity of the potential employee, the right to work in the country, and verification of the last 3 years of employment through reference uptake, it also covers a criminal record check, where allowed.

Corporate Traveller also have policies on what must be performed 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 and Privacy 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 across all employees. The training is updated annually to include the topical high risks facing organisations globally.

## Asset Management

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

# Control Set Statements contin.

## Access Control

Corporate Traveller operate 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. Corporate Traveller have 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.

## Cryptography

Corporate Traveller encrypt all client data at rest and in transit in our systems and networks, and have a policy for key management and storage. We regularly review our standards and ensure our encryption keys are not depreciated.

Corporate Traveller also operate 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 portable devices that have access to Corporate Traveller data must be encrypted. Corporate Traveller utilise products such as Microsoft InTune, Airwatch, and Bitlocker to help achieve these control objectives.

## Physical and Environmental Security

Corporate Traveller also have Physical and Environmental Policies to protect our assets both physical and logical. This 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.

## Operations Security

Corporate Traveller have defined roles and responsibilities for the protection and maintenance of operational security and privacy 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 ensures suitable backup and disaster recovery processes are in place and regularly tested.

Corporate Traveller have a robust approach to vulnerability management with the technology landscape regularly scanned and patches promptly applied based on risk.

## Communications Security

Corporate Traveller have 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.

# Control Set Statements contin.

## System Acquisition Development and Maintenance

Corporate Traveller have 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.

Corporate Traveller have 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 Snyk. Developers are subject to annual secure development training, using products such as Secure Code Warrior.

## Supplier Relationships

The acquisition of any new system is subject to a security and privacy review conducted by the Corporate Security and Privacy teams.

Corporate Traveller operate 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 on 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.

## Information Security Incident Management

Corporate Traveller have 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. FCTG has rolled out our endpoint detection and response capability across our business globally.

## Business Continuity Management

Corporate Traveller have well 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 of our systems are cloud based to ensure that in the case of any disaster that affects a project team, all of our essential tools are accessible so that it is BAU for our teams. All third party systems are also required to have their own BCP capability, as part of our supplier agreements.

## Compliance

Within the departments of both the Group CISO and the Group CPO there are assigned Privacy, Compliance and Assurance roles across the globe, in regard to Information Security and privacy.

The legal department, are based in all geographies and are responsible for tracking and ensuring compliance with local legislative requirements.

# Document Information

| Version | Date | Comments |
|---|---|---|
| 1.0 | Nov 2019 | Initial version |
| 2.0 | Feb 2024 | Update following intention to implement ISO27001 |