



# Information Protection Management System

– FCM Network

[fcmtravel.com](http://fcmtravel.com)

**FCM**





## Our goal

FCM is the flagship global corporate travel business of the Flight Centre Travel Group.

FCM and the Flight Centre Travel Group are committed to protecting confidential and personal information, which we hold or process on behalf of our clients, employees, vendors and other stakeholders. As such, we implement practices to comply with data protection requirements across the entire Group.

Compliance with data protection laws requires close cooperation between FCM and each of our partners. As a global brand, FCM has implemented an integrated global programme to ensure a robust and consistent approach to information protection across our network.

We have developed this Information Protection Management System (“**IPMS**”) so that personal information handled by our partner network is secure and processed in accordance with the information security standards expected by our clients and required by applicable data protection laws around the world. Our goal is to support and encourage the proper handling and use of information processed by the FCM network and to ensure sustainable compliance with our legal obligations to protect personal information.

---

### Purpose of this document

Information security is one of FCM’s key priorities.

Reasonable and ongoing due diligence of our partner network forms an important and integral part of our commitment to clients and is a requirement under data protection laws.

#### **This IPMS should be read in conjunction with:**

- the confidentiality and data processing terms set out in each partner’s licence agreement and/or data processing agreement;
- the minimum technical and organisational measures (“**TOMs**”) set out in the appendix to this document; and
- applicable data protection laws to which each partner is bound, (together, the “**Information Security Standards**”).

This IPMS sets out the structures and systems we utilise to assist us in reviewing our partners’ compliance with the Information Security Standards. It is intended that this document should be distributed to the FCM partner network and may be made available to clients to evidence FCM’s commitment to information security due diligence.

---

## Overview of the IPMS process

We assess our partner network's compliance with the Information Security Standards using different assessment types as determined by risk assessment outputs. Higher levels of identified risk require increased assessments and remediation actions. The various assessment types are described below from lightest touch onwards - encompassing desktop security assessments, on-site security assessments, and the intervention of an FCM Escalation Panel. The risk assessment methodology employed is also described in this IPMS.

---

### Desktop security assessment

A desktop assessment is a high-level documentary review that does not require a physical on-site visit to a partner's office or access to the partner's systems.

Desktop security assessments will be performed in relation to an FCM partner on an ad-hoc basis and carried out by a delegate authorised by Flight Centre Travel Group's Chief Information Security Officer, a Data Protection Officer or Enterprise Risk (an "**Assessor**"). Assessors will review responses to security questionnaires, records, policies, certificates, PCI-DSS attestations and other documents as provided by a partner to the Assessor for the purposes of evaluating the partner's compliance with the Information Security Standards. An Assessor may request that a partner provide further information as is reasonably required to complete the assessment.

Once completed, FCM will take a risk-based approach to working with the partner in an advisory capacity to rectify any identified defects or take such further steps as may be required (including without limitation, conducting a full on-site assessment of the partner's security system).

---

### On-site security assessment

On-site security assessments may be carried out by an Assessor where the results of a desktop assessment do not provide sufficient evidence of compliance with the Information Security Standards, or where FCM otherwise considers that an on-site assessment is necessary (which may include, for example, randomised tests of partner network security).

On-site security assessments will involve a physical visit to the partner's premises and other data processing locations and may include technical security testing (e.g. ethical hacking) of the partner's security system.

FCM will give the partner reasonable notice of any on-site assessment and shall endeavour to avoid causing disruption to the partner's business in the course of such assessment.

---

### Escalation Panel

FCM has set up an Escalation Panel to review extreme and major information security risks identified in the partner network and to consider more generally any issues escalated by an Assessor. The Escalation Panel also provides an oversight capability to ensure consistency in the risk assessment process undertaken by Assessors.

**The Escalation Panel comprises the following senior stakeholders from FCM:**

- Global Managing Director of FCM
- Regional Manager – Partner Programmes in Corporate
- GM Enterprise Risk – Flight Centre Travel Group
- Group Chief Information Security Officer – Flight Centre Travel Group

Recommendations of the Escalation Panel are logged in a risk register maintained by FCM. The Escalation Panel has broad discretion to recommend appropriate corrective action or other mitigation measures to reduce or manage information security risks in the FCM network.



## Risk assessment

A partner will have a potential defect in its information security systems if the results of an assessment indicate a possible non-compliance with the Information Security Standards.

Not all defects carry the same degree of risk to the protection and integrity of personal data. For example, defects that carry an extreme risk may require immediate attention and escalation, whereas defects that carry a minor risk may, in some situations, not require any action.

To aid in the assessment of risk and to increase visibility around the decision making process, an Assessor may utilise a security risk matrix. A security risk matrix is a method of prioritising risk severity and probability to estimate the magnitude of potential impact on individuals. A score in relation to an identified defect may be assigned by an Assessor or the Escalation Panel utilising all available evidence, including desktop or on-site assessment results, records, inspections and recommendations of subject matter experts.

Risk Score(1-5)	Likelihood, chance or probability	Consequence, impact, outcome or severity
5	<b>Almost Certain</b> (a very high probability that it will occur, could occur several times per year)	<b>Catastrophic</b> (complete loss or breach of all personal data held in relation to all clients and individuals)
4	<b>Likely</b> (will probably occur, likely to happen once per year)	<b>Major</b> (loss or breach of personal data including special category data which will cause significant consequences for individuals, affecting all or most clients)
3	<b>Possible</b> (reasonable likelihood that it may arise once in a 5-year period)	<b>Moderate</b> (loss or breach of personal data where individuals may encounter significant inconveniences, affecting all or most clients)
2	<b>Unlikely</b> (plausible, could occur once over a 5-10 year period)	<b>Minor</b> (loss or breach of personal data, where individuals may encounter small inconveniences, not affecting all clients)
1	<b>Rare</b> (very unlikely but not impossible, unlikely in a 10 year period)	<b>Insignificant</b> (loss or breach of personal data where individuals will not be affected)

A risk score is determined by multiplying the likelihood value by the consequence value (e.g. a “possible likelihood” x “major consequence” would have a risk score of 3 x 4 = 12). The risk score is then applied to the risk matrix below:

	5	4	3	2	1
1	Extreme (25)	Extreme (20)	Extreme (15)	Major (10)	Medium (5)
2	Extreme (20)	Extreme (16)	Major (12)	Major (8)	Medium (4)
3	Extreme (15)	Major (12)	Major (9)	Medium (6)	Minor (3)
4	Major (10)	Major (8)	Medium (6)	Medium (4)	Minor (2)
5	Medium (5)	Medium (4)	Minor (3)	Minor (2)	Minor (1)

---

## How we manage the risk for each profile:

Risk	Response
<b>Extreme</b>	Defect to be immediately logged and reported to the Escalation Panel. Corrective action or other appropriate mitigation steps to be taken as a matter of priority.
<b>Major</b>	Defect to be logged and potentially reported to the Escalation Panel. Prompt corrective action or other appropriate mitigation steps to be taken.
<b>Medium</b>	Defect to be logged and corrective action or other appropriate mitigation steps to be taken in due course.
<b>Minor</b>	Defect to be logged and non-urgent corrective action or mitigation steps may be considered.

**Note:** Not all identified defects will necessarily require the allocation of a risk score.

---

## How we work with partners

### Data protection is each partner's responsibility

To ensure the ongoing confidentiality, integrity, availability and resilience of partner systems and services, each partner must meet the Information Security Standards and must implement, at a minimum, the TOMs as set out in the Appendix and such other legal and technical requirements as appropriate to:

- the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage; and
- the nature of the personal data to be protected.

FCM will work with partners in an advisory capacity to recommend policies, procedures and third party products or services to assist the partner in meeting its legal obligations. In the event that a partner delays rectification of an identified defect, the issue may be submitted to the Escalation Panel for further consideration.

---

## Data breaches and incident responses

Each partner must have in place an information security incident management plan to ensure that it reacts appropriately to any actual or suspected security incidents that could affect the confidentiality, integrity, availability and resilience of their systems and services.

A partner must immediately notify FCM of any incident (including an incident relating to its sub-processors) which has resulted or may result in a personal data breach or which otherwise has an adverse effect on the security of client personal data, including but not limited to:

- actual or suspected unauthorised access, disclosure, loss, download, theft, blocking, encryption or deletion by malware or other unauthorised action in relation to personal data by unauthorised third parties; and
- operational incidents which may have an impact on the processing of personal data.

Notification must be made by email to the applicable Flight Centre Travel Group Data Protection Officer at:

- **EMEA:** [data.protection@flightcentre.co.uk](mailto:data.protection@flightcentre.co.uk)
- **AUS/NZ:** [privacy@flightcentre.com.au](mailto:privacy@flightcentre.com.au)
- **Asia:** [dataprotection@flightcentre.com.sg](mailto:dataprotection@flightcentre.com.sg)
- **Americas:** [privacy@am.flightcentre.com](mailto:privacy@am.flightcentre.com)



# Appendix – technical and organisational measures

## 1. Data Security Governance

Partner maintains internal organisational and governance procedures to appropriately manage information throughout its lifecycle. Partner regularly tests, assesses and evaluates the effectiveness of its Information Security Standards.

## 2. Physical Access Control

Partner uses a variety of measures appropriate to the function of the location to prevent unauthorised access to the physical premises where personal data are processed. Those measures include:

- Centralised key and code management, card-key procedures
- Batch card systems including appropriate logging and alerting mechanisms
- Surveillance systems including alarms and, as appropriate, CCTV monitoring
- Receptionists and visitor policies
- Locking of server racks and secured equipment rooms within data centres

## 3. Virtual access control

Partner implements appropriate measures to prevent its systems from being used by unauthorised persons. This is accomplished by:

- Individual, identifiable and role-based user account assignment
- Role-based and password protected access and authorisation procedures
- Centralised, standardised password management and password policies (minimum length/characters, change of passwords)
- User accounts are disabled after excessive failed log-on attempts
- Automatic log-off in case of inactivity
- Anti-virus management

## 4. Data access control

Individuals that are granted use of partner systems are only able to access the data that are required to be accessed by them within the scope of their responsibilities and to the extent covered by their respective access permission (authorisation) and such data cannot be read, copied, modified or removed without specific authorisation. This is accomplished by:


- Authentication at operating system level
- Separate authentication at application level
- Authentication against centrally managed authentication system
- Change control procedures that govern the handling of changes (application or OS) within the environment
- Remote access has appropriate authorisation and authentication
- Logging of system and network activities to produce an audit-trail in the event of system misuse
- Implementation of appropriate protection measures for stored data commensurate to risk, including encryption, pseudonymisation and password controls.

## 5. Disclosure control

Partner implements appropriate measures to prevent data from being read, copied, altered or deleted by unauthorised persons during electronic transmission and during the transport of data storage media. Partner also implements appropriate measures to verify to which entities' data are transferred. This is accomplished by:

- Data transfer protocols including encryption for data carrier/media
- Profile set-up data transfer via secure file transfer methods
- Encrypted VPN
- No physical transfers of backup media





## 6. Data Entry Control

Partner implements appropriate measures to monitor whether data have been entered, changed or removed (deleted), and by whom. **This is accomplished by:**

- Documentation of administration activities (user account setup, change management, access and authorisation procedures)
- Archiving of password-reset and access requests
- System log-files enabled by default
- Storage of audit logs for audit trail analysis

## 7. Instructional Control

Partner implements appropriate measures to ensure that data may only be processed in accordance with the instructions of the client. **Those measures include:**

- Binding policies and procedures on partner employees
- Where sub-processors are engaged in the processing of data, including appropriate contractual provisions to the agreements with sub-processors to maintain instructional control rights

## 8. Availability Control

**Partner maintains appropriate levels of redundancy and fault tolerance for accidental destruction or loss of data, including:**

- Extensive and comprehensive backup and recovery management systems
- Documented disaster recovery and business continuity plans and systems
- Storage and archive policies
- Anti-virus, anti-spam and firewall systems and management including policies
- Data centres are appropriately equipped according to risk, including physically separated back up data centres, uninterruptible power supplies (including backup generators), fail redundant hardware and network systems and alarm and security systems (smoke, fire, water)
- Appropriate redundant technology on data storage systems
- All critical systems have backup and redundancy built into the environment.

## 9. Separation Control

Partner implements appropriate measures to ensure that data that are intended for different purposes are processed separately. **This is accomplished by:**

- Access request and authorisation processes provide logical data separation
- Separation of functions (production / testing)
- Segregation of duties and authorisations between users, administrators and system developers.