Flight Centre (UK) Limited

Technical and Organisational Security Measures

30 December 2019

CT's Technical and Organisational Measures

1. DATA SECURITY GOVERNANCE

CT maintains internal organisational and governance procedures to appropriately manage information throughout its lifecycle. CT regularly tests, assesses and evaluates the effectiveness of its technical and organisational measures.

2. PHYSICAL ACCESS CONTROL

CT 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

CT 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 CT 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**

CT 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. CT 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**

CT 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**

CT implements appropriate measures to ensure that data may only be Processed in accordance with relevant instructions. Those measures include:

- Binding policies and procedures on CT employees
- Where Processors are engaged in the Processing of data, including appropriate contractual provisions to the agreements with Processors to maintain instructional control rights

8. **AVAILABILITY CONTROL**

CT 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**

CT 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 developer.