Information Security Regulation (ISR) Policy

Version 1.0

1 Definitions & Interpretations

The definitions in this section 1 shall apply to this Information Security Regulation (ISR) Policy.

Term	Definition
Agreement	The agreement between flydubai and the Third Party in connection to which the Third Party will access flydubai Data.
Authorised Parties	All persons employed by the Third Party together with the Third Party's agents, representatives and any other party, in each instance, whose engagement and access to flydubai Data is strictly necessary for the performance of the Third Party's obligations under the Agreement.
Business Continuity and Disaster Recovery	A set of processes and techniques used to help an organization recover from a disaster and continue or resume routine business operations.
Confidential Information	Information disclosed by (or on behalf of) a party or its representatives to the other party in connection with the Agreement that is marked as confidential or would reasonably be considered to be confidential under the circumstances.
Dynamic Host Configuration Protocol	A network management protocol used on internet protocol networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.
flydubai	Dubai Aviation Corporation (trading as 'flydubai')

flydubai Data	All information of whatever form relating to flydubai, its business or customers that is provided by flydubai in connection with the performance of the Third Party's obligations under the Agreement, including any information provided or generated, collected, processed, stored or transmitted in connection with their access to and/or use of the Third Party's obligations under the Agreement.
Incident Management Process	A set of procedures and actions taken to respond to and resolve critical incidents: how incidents are detected and communicated, who is responsible, what tools are used, and what steps are taken to resolve the incident.
Mobile and Portable Devices	Small form factor of a computing device that is designed to be held and used in the hands used to connect to the internet and communicate with others.
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not, including but not limited to personal data for the purpose of the General Data Protection Regulation EU 2016/ 679
Policy	This Information Security Regulation Policy.
Restrictive, Reciprocal, Hereditary or Copyleft licence	A software licence that requires that information necessary for reproducing and modifying such software must be made available publicly to recipients of executable versions of such software including but not limited to General Public Licence (GPL) and Affero General Public Licence (AGPL) .
Security Gateway	A set of control mechanisms between two or more networks having different trust levels which filter and log traffic passing, or attempting to pass, between networks, and the associated administrative and management servers.

Strong Authentication	a method of user verification that is considered robust enough to withstand attacks on the system to which the users are authenticating.
Strong Encryption	The use of encryption technologies with minimum key lengths of 128-bits for symmetric encryption and 1024-bits for asymmetric encryption whose strength provides reasonable assurance that it will protect the encrypted information from unauthorised access and is adequate to protect the confidentiality and privacy of the encrypted information, and which incorporates a documented policy for the management of the encryption keys and associated processes adequate to protect the confidentiality and privacy of the keys and passwords used as inputs to the encryption algorithm.
Technical and Organisational Security Measures	Functions, processes, controls, systems, procedures, and measures that organisations can implement to promote secure processing and storage of personal & confidential data, avoid data breaches, and facilitate compliance with relevant data protection obligations.
Third Party	The Third Party accessing flydubai Data in connection with this policy

1. Organisation of Information Security

Third Party shall, at a minimum:

a. Ensure only Authorised Parties are granted access to flydubai Data.

b. Implement Technical and Organisational Security Measures that are no less rigorous than information security best practices to protect the integrity, availability, and confidentiality of flydubai Data and other non-public information and prevent the unauthorised access, acquisition, disclosure, destruction, alteration, accidental loss, misuse or damage of flydubai Data.

c. Establish, implement, and maintain consistent with industry best practices, policies and a program of organisational, operational, administrative, physical and Technical and Organisational Security Measures appropriate to (1) prevent any access by non-Authorised Parties to flydubai Data in a manner not authorised by the Agreement or this Policy, and (2) comply with and meet all applicable laws and regulations and applicable industry standards.

d. Take reasonable steps to prevent unauthorised access to or loss of flydubai Data and the Third Party obligations under the Agreement, systems, devices or media containing this information.

e. Employ risk assessment processes and procedures to regularly assess systems used to provide Third Party obligations or products to flydubai. Third Party shall remediate such risks as soon as possible and commensurate with the level of risk to flydubai Data given threats known at the time of identification. Operate a process to enable the reporting of risks or suspected incidents to the flydubai security team.

f. Keep records of Authorised Parties and Third Party resources that access, transfer, maintain, store, or process flydubai Data.

g. Conduct comprehensive background checks on all Authorised Parties prior to hire, to the extent permitted by law. The comprehensive background check on individuals shall include, at a minimum, the individual's previous employment history, criminal record, credit history, reference checks, and any additional industry standard background check requirements.

h. Require non-disclosure or confidentiality contractual commitments from Authorised Parties prior to providing them with access to flydubai Data.

i. Ensure that all Authorised Parties who may be performing work under the Agreement or who may have access to flydubai Data are in compliance with these Technical and Organisational Security Measures which shall be evidenced by a written agreement no less restrictive than this Policy.

2. Physical and Environmental Security

Third Party shall, at a minimum:

a. Ensure that all of Third Party's systems and other resources intended for use by multiple users are in secure physical facilities with access limited and restricted to authorised individuals only.

b. Monitor and record, for audit purposes, access to the physical facilities containing systems and other resources intended for use by multiple users used in connection with Third Party's performance of its obligations under the Agreement.

c. Limit and monitor physical access to its facilities only to Authorised Parties

d. Equipment used to store, process or transmit flydubai Data must be physically secured including wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

e. Implement controls to minimise the risk of and protect against physical threats.

f. Protect any device that captures payment card data via direct physical interaction from tampering and substitution by periodically inspecting device surfaces to detect tampering or substitution; provide training for personnel to be aware of attempting tampering or replacement of devices.

3. Access Control

Third Party shall, at a minimum:

a. Separate flydubai's information from Third Party's other customers' data or Third Party's own applications and information either by using physically separate servers or by using logical access controls where physical separation of servers is not implemented.

b. Identify and require appropriate owners to review and approve access to systems used to access, process, manage, or store flydubai Data at least quarterly to remove unauthorised access; and maintain and track access approvals.

c. Remove access to systems managing flydubai Data within 24 hours of Authorised Party terminating its relationship with Third Party ; and maintain reasonable procedures to remove access to such systems within three business days when it is no longer needed or relevant to the performance of their duties. All other user IDs must be disabled or removed after 90 calendar days of inactivity.

d. Restrict system administrator (also known as root, privileged, or super user) access to operating systems intended for use by multiple users only to individuals requiring such high-level access in the performance of their jobs. Use check-out system administrator IDs with individual user log-in credentials and activity logs to manage high security access and reduce high-level access to a highly limited number of users. Require application, database, network, and system administrators to restrict access by users to only the commands, data, systems, and other resources necessary for them to perform Authorised functions. System administrative roles and access lists must be reviewed at least annually.

e. Require Strong Authentication for all non-console administrative access, any remote access, and all administrative access into cloud environments.

4. Identification and Authentication

Third Party shall, at a minimum:

a. Assign unique user IDs to individual users and assign authentication mechanisms to each individual account.

b. Use a documented user ID lifecycle management process including, but not limited to, procedures for approved account creation, timely account removal, and account modification (e.g., changes to privileges, span of access, functions/roles) for all access to flydubai Data and across all environments (e.g., production, test, development, etc.). Such process shall include review of access privileges and account validity to be performed at least quarterly.

c. Restrict all access to flydubai Data to those using a valid user ID and password, and require unique user IDs to employ one of the following: password or passphrase, two-factor authentication, or a biometric value.

d. Require password complexity and meet the following password construction requirements as per flydubai policy: a minimum of eight (8) characters in length for system passwords and four (4) characters for tablet and smartphone passcodes. System passwords must contain three (3) of the following: upper case, lower case, numeric, or special characters.

e. Passwords must also not be the same as the user ID with which they are associated, contain a dictionary word, sequential or repeat numbers, and not be one of the past five passwords.

f. Require password expiration at regular intervals not to exceed ninety (90) days.

g. Mask all passwords when displayed.

h. Limit failed login attempts to no more than five (5) failed logon attempts within 24 hours and lock the user account upon reaching that limit in a persistent state. Access to the user account can be reactivated subsequently through a manual process requiring verification of the user's identity.

i. Verify user's identity and set one-time use and reset passwords to a unique value for each user. Systematically prompt change after first use.

j. Use a secure method for the conveyance of authentication credentials (e.g., passwords) and authentication mechanisms (e.g., tokens or smart cards).

k. Restrict service account and proxy passwords to a 12-character minimum, including upper case, lower case, and numeric characters, as well as special symbols. Change service account and proxy passwords at least annually and after employment termination of anyone with knowledge of the password.

l. Terminate interactive sessions, or activate a secure, locking screensaver requiring authentication, after a period of inactivity not to exceed fifteen (15) minutes.

m. Use an authentication method based on the sensitivity of flydubai Data. Whenever authentication credentials are stored, Third Party shall protect them using Strong Encryption.

n. Configure systems to automatically timeout after a maximum period of inactivity as follows: server (15 minutes), workstation (15 minutes), mobile device (4 hours), Dynamic Host Configuration Protocol (7 days), Virtual Private Network (24 hours).

5. Information Systems Acquisition, Development and Maintenance

Third Party shall, at a minimum:

a. Employ an effective application management methodology that incorporates Technical and Organisational Security Measures into the software development process, and ensure that Technical and Organisational Security Measures, as represented by industry best practices, are implemented by Third Party in a timely manner.

b. Follow industry-standard development procedures, including separation of access and code between non-production and production environments and associated segregation of duties between such environments.

c. Ensure internal information security controls for software development are assessed regularly and reflect industry best practices, and revise and implement these controls in a timely manner.

d. Manage security of the development process and ensure secure coding practices are implemented and followed, including appropriate cryptographic controls, protections against malicious code, and a peer review process.

e. Conduct penetration testing on functionally complete applications before released into production and thereafter, at least once every year and after any significant modifications to source code or configuration that align with OWASP, CERT, SANS Top 25, and PCI-DSS. Remediate any exploitable vulnerabilities prior to deployment to the production environment.

f. Use anonymized or obfuscated data in non-production environments. Never use plain text production data in any non-production environment, and never use Personal Information in non-production environments for any reason. Ensure all test data and accounts are removed prior to production release.

g. Review open or free source code approved by flydubai, software, applications, or services for flaws, bugs, security issues or non-compliance with open or free source licensing terms. Third Party shall notify flydubai in advance of using any open or free source code and, if approved for use by flydubai, provide flydubai with the name, version and URL of the open or free source code. Third Party represents and warrants that (i) any open or free source code it uses in its products or in services shall be licensed under "permissive" open or free source code licenses and not under Restrictive, Reciprocal, Hereditary or Copyleft licenses; (ii) Third Party has the right to freely amend, adapt open or free source code and combine open or free source code or contain open or free source code with proprietary code without placing restrictions on such amendments, adaptions, or combinations or proprietary code that contains open or free source code and how these can be licensed onwards (collectively, "derivative works") and (iii) such derivative works will not be subject to any open or free source licence requiring licensing the derivative work or making it available at no charge to third parties under the open or free source licence terms.

h. Not share any code created under the Agreement, regardless of the stage of development, in any shared or non-private environment, such as an open access code repository, regardless of password protection.

6. Software and Data Integrity

Third Party shall, at a minimum:

a. In environments where antivirus software is commercially available, have current antivirus software installed and running to scan for and promptly remove or quarantine viruses and other malware from any system or device.

b. Separate non-production information and resources from production information and resources.

c. Ensure teams use a documented change control process for all system changes, including back-out procedures for all production environments and emergency change processes. Include testing, documentation, and approvals for all system changes and require management approval for significant changes in such processes.

d. Build and maintain a PCI zone if Third Party processes or stores card holder data.

e. For applications that utilize a database that allows modifications to flydubai Data, have and maintain a database transaction audit logging features enabled and retain database transaction audit logs for a minimum of one (1) year with three months immediately available for analysis.

f. Review software to find and remediate security vulnerabilities during initial implementation and upon any significant modifications and updates.

g. Perform quality assurance testing for the security components (e.g., testing of identification, authentication and authorization functions), as well as any other activity designed to validate the security architecture, during initial implementation and upon any significant modifications and updates.

7. System Security

Third Party shall, at a minimum:

a. Regularly create and update the most recent versions of data flow and system diagrams used to access, process, manage, or store flydubai Data.

b. Actively monitor industry resources (e.g.www.cert.org, www.cert.org and pertinent software vendor mailing lists and websites) for timely notification of all applicable security alerts pertaining to Third Party's systems and other information resources.

c. Effectively manage cryptographic keys by reducing access to keys by fewest number of custodians necessary, storing secret and private cryptographic keys by encrypting with a key at least as strong as the data-encrypting key, and storing separately from the data-encrypting key in a secure cryptographic device, in the fewest possible locations. Change cryptographic keys from default at installation and at least every two years, and securely dispose of old keys.

d. Scan externally-facing and internal systems and other information resources, including, but not limited to, networks, servers, applications and databases, with applicable industry-standard security vulnerability scanning software to uncover security vulnerabilities, ensure that such systems and other resources are properly hardened, and identify any unauthorised wireless networks at least quarterly, and prior to release for applications and for significant changes and upgrades within timeframes resulting from risk analyses based upon reasonable and generally accepted IT policies and standards.

e. Ensure that all of Third Party's systems and other resources are and remain hardened including, but not limited to, removing or disabling unused network and other services and products (e.g., finger, rlogin, ftp, and simple Transmission Control Protocol/Internet Protocol (TCP/IP) services and products) and installing a system firewall, Transmission Control Protocol (TCP) wrappers or similar technology.

f. Deploy one or more Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), or Intrusion Detection and Prevention Systems (IDP) in an active mode of operation that monitors all traffic entering and leaving systems and other resources in conjunction with the Agreement in environments where such technology is commercially available and to the extent practicable.

g. Maintain a risk rating process for vulnerability assessment findings aligned with industry best practices to remediate security vulnerabilities in any system or other resource, including, but not limited to, those discovered through industry publications, vulnerability scanning, virus scanning, and the review of security logs, and apply appropriate security patches promptly with respect to the probability that such vulnerability can be or is in the process of being exploited. Critical vulnerability assessment findings and patches must be remediated immediately upon availability and in no event longer than 7 days after release. High vulnerability assessment findings and patches must be remediated within 30 days of release. Medium & Low vulnerability assessment findings and patches must be remediated within 70 calendar days.

h. Conduct generalized penetration testing internally and externally at least annually and after any significant infrastructure or application upgrade or modification.

i. Remove or disable unauthorised software discovered on Third Party's systems and employ industry standard malware controls, including the installation, regular update and routine use of anti-malware software products on all services, systems and devices that may be used to access to flydubai Data. Use reliable and industry best practice anti-virus software where practicable and ensure such virus definitions remain updated.

j. Maintain up-to-date software on all services, systems and devices that may be used to access flydubai Data, including appropriate maintenance of operating system(s) and successful installation of reasonably up-to-date security patches.

k. Assign security administration responsibilities for configuring host operating systems to specific individuals.

l. Change all default account names and/or default passwords.

8. Monitoring

Third Party shall, at a minimum:

a. Retain log data for flydubai Data logs shall be designed to detect and respond to incidents and include, but not be limited to:

   i. All individual user access to flydubai Data

   ii. All actions taken by those with administrative or root privileges

   iii. All user access to audit trails

   iv. Invalid logical access attempts

   v. Use of and changes to identification and authentication mechanisms

b. Record' Third Parties' primary system activities for systems containing any flydubai Data.

c. Restrict access for security logs to Authorised individuals and protect security logs from unauthorised modification.

d. Implement a change detection mechanism (e.g., file integrity monitoring) to alert personnel to unauthorised modification of critical system files, configuration files, or content files; configure software to perform critical file comparisons weekly.

e. Review, on at least a weekly basis, all security and security-related audit logs on systems containing flydubai Data for anomalies and document and resolve all logged security problems in a timely manner.

f. Daily review all security events, logs of system components storing, processing, or transmitting card holder data, logs of critical system components, and logs of servers and system components performing security functions.

9. Security Gateways

Third Party shall, at a minimum:

a. Require Strong Authentication for administrative and/or management access to Security Gateways, including, but not limited to, any access for the purpose of reviewing log files.

b. Have and use documented controls, policies, processes and procedures to ensure that unauthorised users do not have administrative and/or management access to Security Gateways, and that user authorization levels to administer and manage Security Gateways are appropriate.

c. At least once every six (6) months, ensure that Security Gateway configurations are hardened by selecting a sample of Security Gateways and verifying that each default rule set and set of configuration parameters ensures the following:

    i. Internet Protocol (IP) source routing is disabled,

    ii. The loopback address is prohibited from entering the internal network,

    iii. Anti-spoofing filters are implemented,

    iv. Broadcast packets are disallowed from entering the network,

    v. Internet Control Message Protocol (ICMP) redirects are disabled,

    vi. All rule sets end with a “DENY ALL” statement, and

    vii. Each rule is traceable to a specific business request.

d. Ensure that monitoring tools are used to validate that all aspects of Security Gateways (e.g., hardware, firmware, and software) are continuously operational.

e. Ensure that all Security Gateways are configured and implemented such that all non-operational Security Gateways shall deny all access.

f. Inbound packets from the untrusted external network must terminate within the demilitarized zone (“DMZ”) and must not be allowed to flow directly through to the trusted internal network. All inbound packets which flow to the trusted internal network must only originate within the DMZ. The DMZ must be separated from the untrusted external network by use of a Security Gateway and must be separated from the trusted internal network by use of either:

    i. another Security Gateway, or

    ii. the same Security Gateway used to separate the DMZ from the untrusted external network, in which case the Security Gateway must ensure that packets received from the untrusted external network are either immediately deleted or if not

deleted are routed only to the DMZ with no other processing of such inbound packets performed other than possibly writing the packets to a log.

g. The following must only be located within the trusted internal network:

   i. Any flydubai Data stored without the use of Strong Encryption,

   ii. The official record copy of information

   iii. Database servers,

   iv. All exported logs, and

   v. All environments used for development, test, sandbox, production, and any other such environments; and all source code versions.

h. Authentication credentials not protected by the use of Strong Encryption must not be located within the DMZ.

10. Network Security

Third Party shall, at a minimum:

a. Upon flydubai's request, provide to flydubai a logical network diagram documenting systems and connections to other resources including routers, switches, firewalls, IDS systems, network topology, external connection points, gateways, wireless networks, and any other devices that shall support flydubai.

b. Maintain a formal process for approving, testing, and documenting all network connections and changes to the firewall and router configurations. Configure firewalls to deny and log suspicious packets, and restrict to only allow appropriate and authorised traffic, denying all other traffic through the firewall. Review firewall rules every six months.

c. Install a firewall at each Internet connection and between any DMZ and the internal network zone. Any system storing Personal Information must reside in the internal network zone, segregated from the DMZ and other untrusted networks.

d. Monitor firewall at the perimeter and internally to control and protect the flow of network traffic entering or leaving the border or boundary, as necessary.

e. Maintain a documented process and controls in place to detect and handle unauthorised attempts to access flydubai Data.

f. When providing Internet-based services and products to flydubai, protect flydubai Data by the implementation of a network DMZ. Web servers providing services to flydubai shall reside in the DMZ. Any system or information resource storing flydubai Data (such as application and database servers) shall reside in a trusted internal network. Third Party shall use DMZ for Internet services and products.

g. Restrict unauthorised outbound traffic from applications processing, storing or transmitting flydubai Data to IP addresses within the DMZ and Internet.

h. When using radio frequency (RF) based wireless networking technologies to perform or support services and products for flydubai, Third Party shall ensure that all of flydubai Data transmitted is protected by the use of appropriate encryption technologies sufficient to protect the confidentiality of flydubai Data; provided, however, that in any event such encryption shall use no less than key lengths of 256-bits for symmetric encryption and 2048-bits for asymmetric encryption. Regularly scan, identify, and disable unauthorized wireless access points.

11. Connectivity Requirements

In the event that Third Party has, or shall be provided, connectivity to flydubai Data resources in conjunction with the Agreement, then in addition to the foregoing, if Third Party has or is provided connectivity to flydubai's environment, Third Party shall, at a minimum:

a. Use only the mutually agreed upon facilities and connection methodologies to interconnect flydubai's environment with Third Party's resources.

b. NOT establish interconnection to flydubai's environment without the prior written consent of flydubai.

c. Provide flydubai access to any applicable Third Party facilities during normal business hours for the maintenance and support of any equipment (e.g., router) provided by flydubai under the Agreement for connectivity to flydubai Data resources.

d. Use any equipment provided by flydubai under the Agreement for connectivity to flydubai's environment only for the furnishing of those services and products or functions explicitly authorised in the Agreement.

e. If the agreed upon connectivity methodology requires that Third Party implement a Security Gateway, maintain logs of all sessions using such Security Gateway. These session logs must include sufficiently detailed information to identify the end user or application, origination IP address, destination IP address, ports/service protocols used and duration of access. These session logs must be retained for a minimum of six (6) months from session creation.

f. Immediately suspend or terminate any interconnection to flydubai's environment upon Third Parties belief there has been a breach or unauthorised access or upon flydubai's instructions if flydubai, in its sole discretion, believes there has been a breach of security or unauthorised access to or misuse of flydubai Data facilities or any flydubai information, systems, or other resources.

12. Mobile and Portable Devices

Third Party shall, at a minimum:

a. Use Strong Encryption to protect flydubai Data transmitted using or remotely accessed by network-aware Mobile and Portable Devices.

b. When using network aware Mobile and Portable Devices that are not laptop computers to access and/or store flydubai Data, such devices must be capable of deleting all stored copies of flydubai Data upon receipt over the network of a properly authenticated command. (Note: Such capability is often referred to as a "remote wipe" capability.)

c. Have documented policies, procedures and standards in place to ensure that the Authorised Party who should be in physical control of a network-aware mobile and portable device that is not a laptop computer and that is storing flydubai Data promptly initiates deletion of all flydubai Data when the device becomes lost or stolen.

d. Have documented policies, procedures and standards in place to ensure that Mobile and Portable Devices that are not laptop computers and are not network aware shall automatically delete all stored copies of flydubai Data after consecutive failed login attempts.

e. Have documented policies, procedures and standards in place which ensure that any Mobile and Portable Devices used to access and/or store flydubai Data:

   i. Are in the physical possession of Authorised Parties;

   ii. Are physically secured when not in the physical possession of Authorised Parties; or

   iii. Have their data storage promptly and securely deleted when not in the physical possession of an Authorised Party, or physically secured, or after 10 unsuccessful access attempts.

f. Prior to allowing access to flydubai Data stored on or through the use of Mobile and Portable Devices, Third Party shall have and use a process to ensure that:

   i. The user is an Authorised Party authorised for such access; and

   ii. The identity of the user has been authenticated.

g. Implement a policy that prohibits the use of any Mobile and Portable Devices that are not administered and/or managed by Third Party or flydubai to access and/or store flydubai Data.

h. Review, at least annually, the use of and controls for all Third Party-administered or managed Mobile and Portable Devices to ensure that the Mobile and Portable Devices can meet the applicable Technical and Organisational Security Measures.

13. Security in Transit

Third Party shall, at a minimum:

a. Use Strong Encryption for the transfer of flydubai Data outside of flydubai-controlled or Third Party-controlled networks or when transmitting flydubai Data over any untrusted network.

b. For records containing flydubai Data in paper format, microfiche, or electronic media to be physically transferred, transport them by secured courier or other delivery method that can be tracked, packed securely and per manufacturer specifications. Any flydubai Data must be transported in locked containers.

14. Security at Rest

Third Party shall, at a minimum:

a. Use Strong Encryption to protect flydubai Data when stored.

b. Not store flydubai Data electronically outside of Third Party's network environment (or flydubai's own secure computer network) unless the storage device (e.g., backup tape, laptop, memory stick, computer disk, etc.,) is protected by Strong Encryption.

c. Not store flydubai Data on removable media (e.g., USB flash drives, thumb drives, memory sticks, tapes, CDs, or external hard drives) except: for backup, business continuity, disaster recovery, and data interchange purposes as allowed and required under contract between Third Party and flydubai. If removable media is used to store Personal Information or Confidential Information per the exceptions noted within this subsection, the information must be protected using Strong Encryption. Autorun shall be disabled for removable media and storage devices.

d. Appropriately store and secure records containing flydubai Data in paper format or microfiche in areas to which access is restricted to authorised personnel.

e. Unless otherwise instructed by flydubai in writing, when collecting, generating or creating flydubai Data in paper form and backup media for, through or on behalf of flydubai or under the flydubai brand, ensure that such information shall be Personal Information or Confidential Information and, whenever practicable, label such information of flydubai as "Confidential". Third Party acknowledges that flydubai Data is and shall remain owned by flydubai- irrespective of labeling or the absence thereof.

15. Return, Retention, Destruction, and Disposal

Third Party shall, at a minimum:

a. At no additional charge to flydubai, upon flydubai's request or upon termination of the Agreement, provide copies of any of flydubai Data to flydubai within thirty (30) calendar days of such request or termination of the Agreement. Third Party shall return or, at flydubai's option, destroy all of flydubai's data, including electronic, hard, and secured backup copies as provided for in the Agreement or, if not provided for in the Agreement, within ninety calendar (90) days after the soonest of: (i) expiration or termination of the Agreement, (ii) flydubai's request for the return of flydubai Data, or (iii) the date when Third Party no longer needs flydubai Data to perform its obligations and products under the Agreement.

b. In the event that flydubai approves destruction as an alternative to returning flydubai Data, certify in writing, by an officer of the Third Party, the destruction as rendering flydubai Data non-retrievable and unrecoverable. Third Party shall completely destroy all copies of flydubai Data at all locations and in all systems where flydubai Data is stored, including but not limited to previously approved Authorised Parties. Such information shall be destroyed following an industry standard procedure for complete destruction such as DOD 5220.22M or NIST Special Publication 800-88 or using a manufacturer-recommended degaussing product for the system affected. Prior to such destruction, Third Party shall maintain all applicable Technical and Organisational Security Measures to protect the security, privacy and confidentiality of flydubai Data.

c. Dispose of Personal Information and flydubai Confidential Information in a manner that ensures the information cannot be reconstructed into a usable format. Papers, slides, microfilm, microfiche and photographs must be disposed by cross-shredding or burning. Materials containing flydubai Data awaiting destruction must be stored in secured containers and be transported using a secure third party.

16. Incident Response and Notification

Third Party shall, at a minimum:

a. Have and use an Incident Management Process and related procedures and staff such Incident Management Process and procedures with specialized resources. Immediately, and in no event more than twenty-four (24) hours, notify flydubai whenever there is any suspected or confirmed attack upon, intrusion upon, unauthorised access to, loss of, or other incident regarding flydubai's information, systems, or other resources.

b. After notifying flydubai, provide flydubai with regular status updates, including, but not limited to, actions taken to resolve such incident, at mutually agreed upon intervals or times for the duration of the incident and as soon as reasonably possible after the closure of the incident, provide flydubai with a written report describing the incident, actions taken by the Third Party during its response and Third Party's plans for future actions to prevent a similar incident from occurring.

c. Not report or publicly disclose any such breach of flydubai's information, systems, or other resources without first notifying flydubai and working directly with flydubai to notify applicable regional, country, state, or local government officials or credit monitoring services, individuals affected by such breach, and any applicable media outlets, as required by law.

d. Have a process in place to promptly identify violations of security controls including those set forth in this Policy by Third Parties. Identified violators shall be subject to appropriate disciplinary action subject to the applicable laws. Notwithstanding the foregoing, violators shall remain under the authority of the Third Parties. flydubai shall not be deemed employer of the Third Party.

17. Business Continuity Management and Disaster Recovery

Third Party shall, at a minimum:

a. Develop, operate, manage, and revise business continuity plans for each location and disaster recovery plans for each core technology in order to minimise impact on flydubai attributable to the Third Party's performance of its obligations under the Agreement. Such plans shall include: named resources specific to Business Continuity and Disaster Recovery functions, established recovery time objectives and recovery point objectives, daily back-up of data and systems, off-site storage of backup media and records, record protection and contingency plans commensurate with the requirements of the Agreement, store such plans securely off-site and ensure such plans are available to Third Party as needed.

b. Upon flydubai's request, furnish to flydubai a documented business continuity plan that ensures Third Party can meet its contractual obligations under the Agreement and this document, including the requirements of any applicable statement of work or service level agreement. Such plans shall exercise recovery while protecting integrity and confidentiality of flydubai Data.

c. Have documented procedures for the secure backup and recovery of flydubai Data which shall include, at a minimum, procedures for the transport, storage, and disposal of the backup copies of flydubai Data and, upon flydubai's request, provide such documented procedures to flydubai.

d. Ensure that backups of all flydubai Data stored or software and configurations for systems used by flydubai are created at least once a week.

e. Regularly, but no less frequently than annually, or following any material change in business continuity or disaster recovery plans, comprehensively exercise such plans at Third Party's sole cost and expense. Such exercises shall ensure proper functioning of impacted technologies and internal awareness of such plans. Business Continuity and Disaster Recovery plans shall be updated at least annually, or as often as necessitated by significant changes to the business and/or technology environment.

f. Promptly review its business continuity plan to address additional or emerging threat sources or scenarios and provide flydubai a high-level summary of plans and testing within a reasonable timeframe upon request.

g. Ensure that all Third Party or Third Party-contracted locations housing or processing flydubai Data are monitored 24 hours a day, seven (7) days per week against intrusion, fire, water, and other environmental hazards.

18. Compliance and Accreditations

Third Party shall, at a minimum:

a. Retain complete and accurate records relating to its performance of its obligations arising out of this Policy and Third Party's compliance herewith in a format that shall permit assessment or audit for a period of no less than three (3) years or longer as may be required pursuant to a court order or civil or regulatory proceeding. Notwithstanding the foregoing, Third Party shall only be required to maintain security logs for a minimum of one (1) year after any continuing performance of the Agreement.

b. Allow flydubai, at no additional cost to flydubai, upon reasonable advance notice, conduct periodic security assessments or audits of the Technical and Organisational Security Measures used by Third Party during which flydubai shall provide Third Party with written questionnaires and requests for documentation. For all requests, Third Party shall respond with a written response and evidence, if applicable, immediately or upon mutual agreement. Upon flydubai's request for an audit by flydubai, Third Party shall schedule a security audit to commence within ten (10) business days from such request. flydubai may require access to facilities, systems, processes, or procedures to evaluate Third Party's security control environment.

c. Upon flydubai's request, certify it is in compliance with this document along with supporting certifications for the most recent versions of PCI-DSS, ISO 27001/27002, SOC 2, or similar assessment for the Third Party and for any subcontractor or third-party processing, accessing, storing, or managing on behalf of the Third Party. If Third Party is not able to certify compliance, it shall provide a written report detailing where it is out of compliance and its remediation plan to become compliant.

d. In the event that flydubai, in its sole discretion, deems that a security breach has occurred which was not reported to flydubai in compliance with this Agreement and Third Party's Incident Management Process, schedule the audit or assessment to commence within twenty-four (24) hours of flydubai's notice requiring an assessment or audit.

e. Within thirty (30) calendar days of receipt of the assessment results or audit report, provide flydubai a written report outlining the corrective actions that Third Party has implemented or proposes to implement with the schedule and current status of each corrective action. Third Party shall update this report to flydubai every thirty (30) calendar days reporting the status of all corrective actions through the date of implementation. Third Party shall implement all corrective actions within ninety (90) days of Third Party's receipt of the assessment or audit report or within an alternative time period provided such alternative time period has been mutually agreed to in writing by the parties within no more than thirty (30) days of Third Party's receipt of the assessment or audit report.

f. Be currently compliant and continue to be compliant with any applicable government mandated information security standards and reporting requirements and ISO 27001/27002. To the extent that Third Party handles payment account numbers or any other related payment information, Third Party shall be currently compliant with the most current version of Payment Card Industry (PCI-DSS) for the full scope of systems handling this information and continue such compliance. In the event Third Party no longer is compliant with PCI-DSS for any portion of the full scope of systems handling PCI-applicable data, Third Party will promptly notify flydubai, immediately proceed without undue delay to remedy such non-compliance, and provide regular status of such remediation to flydubai upon request.

19. Standards, Best Practices, Regulations, and Laws

In the event Third Party processes, accesses, views, stores, or manages flydubai Data pertaining to flydubai personnel, partners, affiliates, flydubai clients; or flydubai client employees, contractors, subcontractors, or suppliers; Third Party shall employ Technical and Organisational Security Measures no less strict than is required by applicable global, regional, country, state, and local guidelines, regulations, directives and law.