Carnival Corporation and plc
Vendor Security Specifications

Definitions As used herein, the following terms shall have the meanings set forth below:

- **"Carnival"** means Carnival Corporation, Carnival plc and/or any of their respective subsidiaries, affiliates or divisions, as applicable (individually or collectively).
- **"Confidential Information"** has the meaning given to such term, including such other similar terms with similar intent, by Vendor's agreement with Carnival.
- **"Personal Data"** has the meaning given to such term, including such other similar terms with similar intent, by applicable data protection and/or privacy law.
- **"Vendor"** means any vendor, service provider, supplier, business partner or other counterparty or signatory to an agreement with Carnival, as applicable.

1.	**Governance and Policies**	• Maintain written information security policies and procedures and incident response programs required to comply at a minimum with (i) all applicable Data Protection Laws and (ii) generally accepted industry standards for data protection including ISO 27001:2013 • Obligation to align with the ISO 27002:2013 security standard or above • Test its information security procedures and incident response programs at least annually and retain written reports of the test results • Assign personnel with responsibility for the determination, review and implementation of security policies and measures
2.	**Network level security**	Measures employed to prevent unauthorized access to the processing environment and thwart attackers from breaching the Vendor's network. Security measures may include technology in the following categories: • Perimeter next generation firewalls and VPN-based access controls to protect the private service networks and back-end servers • Denial of Service protection • Data loss prevention • Advanced Persistent Threat detection/prevention • Mobile device management • Web application security • Continuously monitoring infrastructure security • Regularly examining security risks by internal employees and third-party auditors • Role-based access control implemented in a manner consistent with principle of least privilege • Remote access secured by using various two-factor authentication tokens, or multi-factor authentication

3.	**Intrusion, anti-virus and anti-malware**	Defenses deployed on systems used to process Confidential Information or Personal Data. • Implement patch management procedures that prioritize security patches for systems used to process Carnival Confidential Information or Personal Data • Maintain logs of all auditing, monitoring, and security activity for a period of 120 days in a secure environment • Employ anti-virus, endpoint protection and response capabilities
4.	**Cloud hosting**	Where any part of the Services is supported by cloud hosting, Vendor will comply with the latest version of the Cloud Security Alliance Cloud Controls Matrix (available here: https://cloudsecurityalliance.org) or other substantially similar assurance agreed with Carnival. Vendor must be able to demonstrate the established commonly accepted data protection and privacy control objectives.

5.	**Physical Site Security and Device Hardening**	Security Measures in place as applicable to at the location where Confidential Information or Personal Data will be processed or stored. Established security areas: • Electronically locked doors • Electronic access card reading system • Management of keys/documentation of key holders • Solid reinforced concrete exterior to building with no windows. • 24x7x365 staffed security guards • Security service, front desk with required sign in for all visitors • Burglar alarm system • Internal and external infrared pan, tilt, zoom CCTV Monitored building management system • Biometric scanners • Remove unused software and services from devices used to Process Confidential Information or Personal Data. • Default passwords that are provided by hardware and software producers shall not be used • Mandate and ensure the use of system enforced strong passwords in accordance with leading industry practices on all systems hosting, storing, processing, or that have or control access to Carnival's information and • Passwords and access credentials are kept confidential and not shared among personnel.

6.	**Access control**	Measures taken for preventing data processing systems from being used without authorization. • Personal and individual user log-in when entering the system and/or the corporate network • Password procedures minimum of 8 characters, with one upper case, lower case, and digit. If the user account has five invalid logon attempts, the account will be locked out. All passwords expire after 90 days. Upon verification of the username and password, the application uses session-based token authentication. • Remote access for maintenance requires two-factor authentication • Automated screen locks after a defined period of inactivity • Password protected screen savers • All passwords are electronically documented and protected against unauthorized access through encryption • User accounts are audited twice per year

7.	**Virtual access control.**	Measures taken to ensure that persons entitled to use a data processing system have access only to Confidential Information or Personal Data to which they have a right of access, and that Confidential Information or Personal Data cannot be read, copied, modified, or removed without authorizations while processing or use and after storage. • User authentication is based on username and strong password • Data are stored encrypted at rest • All transactional records contain identifiers to distinguish client records • System processing uses a role-based mechanism to tailor data access to specific users and roles • Data access, insert, and modification are logged • ISO certifications and/or Third-Party Independent audit reports are maintained at the primary data center
8.	**Cardholder data processing**	When processing or accessing cardholder data on Carnival's behalf, Vendor must adhere to the applicable credit card handling standards per card issuer. Vendor must be compliant with Payment Card Industry Data Services Standard ("PCI-DSS") and will provide proof of compliance annually.

9.	**Transmission control**	Measures taken to ensure that Confidential Information or Personal Data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Confidential Information or Personal Data by means of data transmission facilities is envisaged. • All data (particularly including Sensitive Personal Data) are encrypted in flight using the latest secured transmission protocols Transport Layer Security (TLS) 1.3 with a 2048-bit RSA key exchange or above • Access to reports is logged • Backup media are encrypted • Removable storage is not used
10.	**Input control measures**	Taken to ensure that it is possible to check and establish whether and by whom Confidential Information or Personal Data have been entered into data processing systems, modified, or removed. • Utilization of user identification credentials • Record entry is restricted to a defined set of roles • All entry is date/time stamped and includes identifiers for entering party • Firewalls and intrusion prevention systems are in place to prevent unauthorized access
11.	**Assignment control**	Employed to ensure that, in the case of commissioned processing of Confidential Information or Personal Data, the data are processed strictly in accordance with the instructions of the principal. • Confidentiality agreements are in place for all individuals with data access • Privacy and information security training is conducted during onboarding and on a regular basis • No third parties used for the processing of data other than as described in Agreements • Privacy policy describes rights and obligations of agent and principal
12.	**Availability control**	Measures taken to ensure that Confidential Information or Personal Data are protected from accidental destruction or loss. • Systems employ redundancies such as RAID arrays & redundant equipment • Backups are stored in alternate location from primary processing • Multiple air conditioning units are installed to provide redundant capacity in an N+1 configuration • High sensitivity smoke detection, and an industry-recognized data center fire suppression system • Multiple firewall layers and virus protection on all servers • UPS backed by N+1 generator • Diverse fiber routing and multiple carriers

13.	**Separation control**	Measures taken to ensure that Confidential Information or Personal Data collected for different purposes can be processed separately. • Three-tier systems are used to physically separate presentation, business processing and storage • Carnival's data is stored in separate databases or in logically separate architectures • Separation of duties is used internally to ensure functions pass through change control processes • Discrete development, staging and production environments are maintained. • All routing of data for processing is controlled through automated rules engines. • Computing and storage are on equipment owned by Vendor
14.	**Communications**	• Systems and processes are in place to communicate cybersecurity incident and response investigation results • Promptly communicate investigation results from cybersecurity incident response to Carnival. • *Contact cyber@carnival.com to inform Carnival.*
15.	**Software Development Controls**	Where services and/or deliverables by Vendor include software development: • Source code is managed via a secure version control system • Secrets i.e. passwords, API keys, etc., are not stored in source code • Source code is subject to regular SAST (static analysis) scans • Software dependencies i.e. code libraries, packages, modules, frameworks subject to SCA (software composition analysis) scans • Development practices and testing methodologies (including the above scanning techniques) take into account common vulnerability vectors and up-to-date vulnerability databases e.g. OWASP Top 10, NIST NVD