Effective Date: June 1, 2018

DETAILED DATA SECURITY SPECIFICATIONS DOCUMENT

For those Suppliers who store, process, transmit or potentially have access to Personal Information, the below Detailed Data Security Specifications document **"DDSS"** shall apply. **"Personal Information"** or "**PII**" means any information relating to an identified or identifiable person and that, either by itself or in combination with other pieces of information, identifies, or can be used to identify, an individual. Examples of Personal Information include, but are not limited to, names, phone numbers, addresses, credit card information, social security numbers, and/or account or financial information of Wyndham's or its affiliates' employees, franchisees, sales associates, brokers, or customers.

I. **Security – Generally.** Supplier shall keep as confidential all confidential and proprietary information of Wyndham's affiliates, employees, franchisees, sales associates, brokers, and customers which is provided to the Supplier (or to which the Supplier has access) ("**Confidential Information**"). If Supplier Processes any Confidential Information, and/or Supplier has access to any Business Systems that Process Confidential Information, Supplier shall at all times comply with Wyndham's and its affiliates' reasonable policies and guidelines for privacy, information protection, and data and systems security, which it has received. Without limiting the generality of the foregoing, Supplier shall maintain (and comply with) a reasonable, comprehensive information security program, which consists of written plans and practices to protect the confidentiality, privacy, integrity and availability of Confidential Information. **"Business Systems"** include, but are not limited to, mainframe computers and terminals, distributed servers, network devices, communication equipment, host or server computers (whether stand-alone or networked), desktops, laptops, software, hand held and other wireless devices (including iPads and Tablets) and personal digital assistants (e.g. BlackBerry), removable electronic media such as USB devices, thumb drives, blue tooth and blue-ray discs, any communications devices, all internal and external communications networks (for example, Internet, Intranet, commercial on-line services, WiFi, VPN, e-mail systems, electronic public folders, and IM programs) that may be accessed directly or indirectly from Wyndham's computers, monitors, docking stations, telephones, headsets, voicemail, copy machines, storage and printing devices, facsimile machines, cameras, video conferencing facilities and other external links, whether on-site, mobile or remote, physical storage systems, and all electronic and analog devices, software, and means of electronic, analog, or physical communication or storage provided or maintained by Wyndham and/or its service providers for business use, or on which any business information is stored, processed, or transmitted. Wyndham Business Systems may also include home or personal computers, laptops, phones, and any other personal communications devices, software, data files or applications and networks, when such systems are used to perform Wyndham business, and/or if those devices are used to store, process, or transmit Wyndham business information. **"Process", "Processing" or "Processed"** means any operation or set of operations that is performed with or upon Confidential Information, whether or not by automatic means, including, but not limited to, receiving, collecting, recording, organizing, storing, accessing, transmitting, adapting, altering, retrieving, consulting, using, disclosing, disseminating, making available, aligning, combining, blocking, deleting, erasing or destroying.

With respect to Confidential Information and systems which Process the same, Supplier shall, upon execution of an appropriate confidentiality agreement between the parties, provide Wyndham with a copy of its written security program documentation, and Supplier shall at minimum:

(i) Use access controls limiting access to only authorized users and preventing unauthorized access through the use of effective physical, technical and administrative access controls including removing access for terminated employees and/or user who no longer need access;

(ii) Limit administrator-level control to only authorized persons;

(iii) Allow only the data protocols required for the function and management of the solution to be transmitted or utilized;

(iv) Ensure the integrity of all data stored or processed;

(v) Prevent the loss of data processed or transferred;

(vi) Assign responsibility and accountability for information security practices and system changes and maintenance;

(vii) Identify, assess, and address reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records, evaluating and improving, where necessary, the effectiveness of safeguards for limiting such risks, including but not limited to: ongoing employee (including temporary and contract employee) training; employee compliance with policies and procedures; and means for detecting and preventing security system failures;

(viii) Develop security policies for employees that take into account whether and how employees should be allowed to physically or electronically store, access and transport records containing PII outside of business premises;

(ix) Train personnel on the security practices and impose disciplinary measures for violations;

(x) If sub-contracting is otherwise allowed, take reasonable steps to verify that Supplier has the legal authority to transfer PII to its subcontractors and service providers, including international and cross-border transfer of PII, as applicable, and such subcontractors and service providers have the capacity to protect applicable information, including testing their security controls and contractually requiring them to maintain such comprehensive data protection safeguards, which shall be no less rigorous than those required by Wyndham of Supplier;

(xi) Limit the collection and retention of information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected;

(xii) Limit distribution of such information to those Supplier personnel with a need-to-know such information necessary to perform the Supplier's obligations under this DDSS;

(xiii) Use Strong Encryption of all Confidential Information stored on laptops or other portable devices, and anytime such information is transmitted wirelessly or otherwise over any open public network, including the Internet. **"Strong Encryption"** means the use of an algorithmic process to transform data into a form in which there is an extremely low likelihood or probability of understanding or assigning meaning to the information without use of a confidential process or key, and which meets or exceeds the definition of "Strong Cryptography" as that term is defined under the Payment Card Industry Data Security Standard;

(xiv) Use reasonable restrictions upon physical access to records, such as using locked facilities, storage areas, and containers;

(xv) Regularly monitor and test its data protection and security plans and procedures to determine whether those protections are reasonably calculated to prevent unauthorized access to, and disclosure of, Confidential Information, upgrading information safeguards as necessary to limit identified risks;

(xvi) Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity and availability of records containing Confidential Information;

(xvii) Document responsive actions taken in connection with any incident involving an Information Security Incident, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Confidential Information. **"Information Security Incident"** means: (a) the loss or misuse (by any means) of Confidential Information; (b) the inadvertent, unauthorized, and/or unlawful Processing, disclosure, access, alteration, transfer, sale or rental, destruction, use, or corruption as a result of unauthorized access, of Confidential Information; or (c) any other act or omission that compromises or threatens to compromise the security, confidentiality, or integrity of Confidential Information coupled with an actual or threatened unauthorized disclosure of that Confidential information; and

(xviii) Use reasonable data protection and information security measures designed to avoid an Information Security Incident.

(xix) Perform comprehensive background checks of all its personnel who will have access to PII.

II. **Technical - Systems - Security Requirements.** Additionally, with respect to Confidential Information and systems which Process the same, Supplier shall at minimum:

(i) Secure user authentication protocols including:

(a) Control of user IDs and other identifiers;

(b) A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(c) Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

(d) Restricting access to active users and active user accounts only; and

(e) Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(ii) Secure access control measures that:

(a) Restrict access to records and files containing Confidential Information to those who need such information to perform their job duties; and

(b) Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(iii) Conduct reasonable monitoring of systems for unauthorized use of or access to Confidential Information;

(iv) Maintain reasonably up-to-date perimeter security devices (e.g. firewall protection) and operating system security patches on systems accessible from open public networks, or otherwise where deemed reasonably necessary to protect Confidential Information;

(v) Maintain reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date security patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and

(vi) Educate and train its employees on the proper use of the computer security system and the importance of information security.

III. <u>Use and Protection of Information</u>.

(i) Additionally, if Supplier Processes Confidential Information, and/or Supplier has access to Business Systems that Process Confidential Information, Supplier shall at all times:

(a) Hold such information in the strictest of confidence;

(b) Immediately (but in no event later than 24 hours) notify Wyndham of any known or suspected Information Security Incident; and, cooperate with Wyndham concerning any disclosures to affected persons or entities and other remedial measures. Additionally, written notification must be sent to Wyndham within forty-eight (48) hours of discovery or notification of such known or suspected Information Security Incident, and such written notification shall describe the potential or probable risk, any known correction or mitigation actions, their impact and a plan for implementing the corrective action selected. In the event that any Information Security Incident arises from the sole act or omission of Supplier, Supplier shall solely bear all expenses, and damages arising from such Information Security Incident, notwithstanding the limitations of liability set forth in any applicable agreement between the parties;

(c) With respect to PII, Process PII only on Wyndham's reasonable instructions and only in accordance with any applicable agreement between the parties for the purposes of performing its obligations under this DDSS, and for no other purpose;

(d) Not create or maintain data which are derivative of Confidential Information except for the purpose of performing its obligations under any applicable agreement between the parties and as authorized in writing by Wyndham; and

(e) Return or destroy (at the election of Wyndham) all Confidential Information, and shall not Process any Confidential Information after being instructed not to do so by Wyndham.

(ii) In the event that Supplier develops software code and/or updates or modifications pursuant to any applicable agreement between the parties, Supplier shall at all times protect all program source code when developing such software code and/or updates or modifications. Supplier shall also test, as appropriate, the security features and controls of all such software and/or updates and modifications and guarantee they are securely coded (for example, ensuring the absence of "backdoors" and hidden keylogger applications). Supplier shall provide Wyndham with written reports of all such testing and the results of the same upon Wyndham's request.

(iii) In the event that the Supplier's obligations under any applicable agreement between the parties involve the collection of PII directly from an individual(s), Supplier shall:

(a) Provide a Privacy Notice to all affected individuals. No Privacy Notices may be displayed unless first approved in advance by Wyndham in writing. **"Privacy Notice"** means notice provided to affected individuals advising that their PII is being collected, processed, stored, used or disclosed, if and when required by applicable law. Such notices will disclose information such as how PII will be

collected, used or disclosed;

(b) Obtain and document meaningful choice and access with respect to use of the PII and provide individuals with the opportunity to authorize, modify, or revoke authorization of use of PII in accordance with instructions of Wyndham or the affected individuals, as applicable;

(c) Only collect and store such PII as required, relevant and reliable to provide or perform its obligations under any applicable agreement between the parties; andProvide appropriate enforcement mechanisms or the investigation and resolution of complaints and disputes by affected individuals, including verifying compliance and remedying non-compliance with Supplier's privacy and security obligations under this DDSS and applicable law.

IV. **Cardholder Data.** To the extent that Supplier stores, Processes, accesses or transmits payment card "Account Data", and specifically "Cardholder Data" and "Sensitive Authentication Data" (as defined by the Payment Card Industry Data Security Standard, hereafter "**PCI DSS**") of Wyndham's or its affiliates' employees or customers, Supplier represents and warrants that it stores, transmits and processes such data in compliance with PCI DSS requirements as well as any other applicable payment standards, or applicable laws and regulations. Supplier further represents and warrants that it shall continue to be fully compliant with all such standards, laws and regulations for all times that it stores, Processes, accesses, or transmits payment card "Account Data". Supplier further acknowledges that it is Supplier's ongoing responsibility hereunder for securing Cardholder Data and Sensitive Authentication Data in accordance with the PCI DSS. Should Supplier fail to maintain compliant practices in accordance with this section, such failure shall be deemed a material breach of any applicable agreement between the parties.

V. **Access to and Security of Wyndham's Networks and Systems.**

Supplier shall not tamper with, compromise, or attempt to circumvent any physical or electronic security or audit measures employed by Wyndham or its affiliates in the course of Wyndham's or its affiliates' business operations. Supplier shall not, without Wyndham's prior express written consent, or as otherwise provided in the applicable agreement between the parties, and without complying with Wyndham's and its affiliates' reasonable policies and guidelines for privacy, information protection, and data and systems security, which it has received, (i) access any Confidential Information or computer systems of Wyndham or its affiliates, or (ii) remove from Wyndham's premises any Confidential Information, or any other property of Wyndham, its affiliates, employees, franchisees, sales associates, brokers or customers. Supplier shall disclose to Wyndham the nature and functions of any electronic means (including, but not limited to, electronic mail, website, and/or the Internet) by which Supplier intends to assist Wyndham in the performance of its obligations under this DDSS and any applicable agreement between the parties. To the extent that Supplier performs any of its obligations under this DDSS and any applicable agreement between the parties via such electronic means, and/or has access to Wyndham's or its affiliates' electronic mail, website, computer systems or networks, and/or other Internet systems, Supplier shall implement and maintain industry-standard security to protect Wyndham's and its affiliates' computer systems, network devices and/or the data processed thereon against the risk of penetration by, or exposure to, a third party via any system or feature utilized by Supplier in performing such work and/or accessing such systems. Such protections shall include, but not be limited to, (a) protecting against client side intrusions, (b) encrypting Confidential Information, (c) securing the computer systems and network devices, and (d) protecting against intrusions of operating systems or software.

Supplier and its agents, employees, or contractors may receive access to Wyndham's Business Systems. Such Business Systems are intended to be used for legitimate business purposes related to Wyndham's business. Accordingly, Supplier acknowledges and agrees as follows:

(i) Supplier shall have no expectation of privacy in its use of or access to Wyndham's Business Systems, and all communications made with such Business Systems or equipment by or on behalf of Supplier are subject to Wyndham's monitoring, recording, inspection, use and disclosure, in Wyndham's discretion;

(ii) Wyndham may, for any business purposes, monitor, review, audit, intercept, access, archive, and/or disclose materials sent over, received by or from, or stored in any of its Business Systems. Without limiting the generality of the foregoing, this includes, without limitation, email communications sent by users across the internet and intranet from and to any domain name owned or operated by Wyndham; and any electronic communication Business Systems that have been used to access any of Wyndham's Business Systems;

(iii) Supplier's use of security measures, as required pursuant to this DDSS and any applicable agreement between the parties to protect Wyndham's Confidential Information (e.g., use of encryption and passwords), does not give Supplier any privacy rights in the communication as between Supplier and Wyndham;

(iv) (d) Wyndham may override any security passwords to obtain access to voicemails, emails, computers (and software or other applications) and/or computer disks on Wyndham's Business Systems;

(v) Wyndham may, for any business purposes, search any and all work areas (for example, offices, cubicles, desks, drawers, cabinets, computers, computer disks and files) and any and all personal items brought onto Wyndham's premises or otherwise used to access Wyndham's Business Systems; and

(vi) Supplier shall provide notice of this monitoring to all of its agents, employees and contractors that may have access to Wyndham's Business Systems.

VI. **Wyndham Audit and Monitoring.** Wyndham reserves the right to audit and/or assess the Services and any Service sites for Supplier's compliance with the Security- Generally, Technical Systems Security Requirements, and Use and Protection of Information Sections of this DDSS. Wyndham shall have the option to assess and/or audit Supplier's privacy and information security practices at least once annually, and at any time after an Information Security Incident caused, or contributed to, by Supplier. Such assessments and audits may include, but are not limited to, assessment of physical, administrative, and technical measures involved with any data centers through which Confidential Information is Processed. Should any such assessment and/or audits reveal any vulnerabilities which are reasonably unacceptable to Wyndham, and should Supplier be unwilling or unable to make any modifications to acceptably reduce or eliminate such vulnerabilities, then Wyndham may terminate any applicable agreement between the parties without penalty. Except as triggered by an Information Security Incident, any audits or assessments of Supplier's physical premises by, or on behalf of, Wyndham shall be (A) permitted only upon no less than 30 days prior written notice; and, (B) performed at Wyndham's sole expense.

VII. **Security Assessments.** In the event Supplier (a) conducts any risk assessments, security assessments or other audits, reviews or assessments (collectively "**Security Assessments**") internally, or (b) obtains any Security Assessments from any outside auditor, consultant or other third-party, Supplier shall provide Wyndham with all reports and other documentation ("**Assessment Documentation**") relating to such Security Assessments no later than thirty (30) days after completion or receipt by Supplier of such Assessment Documentation. Security Assessments may include, but are not limited to, self-assessments, internal audits, SSAE 16 audit reports (i.e.,

Type I or Type II, SOC 1, SOC 2 and/or SOC 3), vulnerability scanning, PCI DSS Self-Assessment Questionnaires (SAQs), PCI DSS Reports on Compliance (ROCs), etc. Wyndham agrees to treat all Assessment Documentation as Confidential Information of Supplier.

VIII. **Removal of Hardware.** In the event that any Services hereunder require Supplier to remove hardware from Wyndham's or its affiliates' premises, Supplier shall use industry standard methods to degauss or destroy all data resident on any such hardware prior to removing such hardware from Wyndham's or its affiliates' premises, or promptly thereafter, and shall within fifteen (15) days of removing such hardware from Wyndham's or its affiliates' premises certify to Wyndham in writing that all such data has been degaussed or destroyed. Additionally, prior to removing any such hardware from Wyndham's or its affiliates' premises for such purposes, Supplier shall verify with Wyndham in writing that Wyndham or the applicable affiliate has backed up all data resident on such hardware.

REVISIONS HISTORY

Revision	Date	Modified By	Modification
1.0	06.01.2018		Initial Version