Data Processing Addendum

This Data Processing Addendum ("DPA") is entered into between Publix Super Markets, Inc., a Florida corporation, having its principal place of business at 3300 Publix Corporate Parkway, Lakeland FL 33811-3311 (together with its subsidiaries and affiliates referred to below as "Publix") and the entity named in the Agreement, including all subsidiaries and affiliates ("Vendor") (each as "Party"; collectively; the "Parties") and effective as of the date of last signature below.

WHEREAS, the Parties have entered into or may in the future enter into one or more agreements (collectively, the "Agreement" for the provision of certain products or services (the "Services") by Vendor to Publix;

WHEREAS, the Parties have agreed that, in connection with the provision of the Services, Vendor may be provided with, use, store, process, access, or otherwise receive Personal Data (as such term is defined below) from or on behalf of Publix;

IN CONSIDERATION OF mutual covenants and agreements set forth below, the Parties, intending to be legally bound, hereby agree as follows:

1. Definitions

1.1.1 "Authorized Users" mean those employees, contractors, or agents of Vendor who are authorized to access Protected Information to perform the Services.

1.1.2 "Data Subject" means an identified or identifiable person to whom Publix Personal Data relates.

1.1.3 "Data Subject Request" means a request from a Data Subject seeking to exercise a right related to their Personal Data, either pursuant to Data Protection Laws or Publix's privacy policy (including requests to exercise any right of access, deletion, correction, opt-out of certain disclosures, or restriction of processing).

1.1.4 "Data Protection Laws" means all applicable laws, rules, regulations, orders, or regulatory guidance relating to data security, data protection, and/or privacy.

1.1.5 "Personal Data" means any information that identifies, relates to, describes, or can be reasonably linked to a person, a household, or a person's device.

1.1.6 "Process" and variations thereof (*e.g.,* "Processing") means any operation or set of operations that are performed on Personal Data and includes, without limitation, the collection, use, storage, disclosure, analysis, deletion, modification, and deidentification of Personal Data.

1.1.7 "Protected Information" means any and all data provided to Vendor by Publix, Publix's subsidiaries and affiliates, or Publix's vendors or that is collected by Vendor on Publix's behalf, including but not limited to any Publix Personal Data.

1.1.8 "Publix Personal Data" means Personal Data that is provided by or on behalf of Publix or is otherwise Processed by Vendor in connection with the performance of the Services.

1.1.9 "Sell" and "Share" have the meanings assigned to those terms in Data Protection Laws.

2. Processing of Personal Data.

2.1 With respect to Publix Personal Data, the Parties agree that Publix is the Controller and Vendor Processes Personal Data as a Processor on behalf of Publix.

2.2 Publix directs Vendor to Process Personal Data during the duration of Vendor's Agreement with Publix for the specific purpose of performing the Services, pursuant to Publix's instructions and details of Processing as set forth at Appendix A.

2.3 Vendor shall Process Publix Personal Data in compliance with all Data Protection Laws. Vendor shall promptly advise Publix if it makes a determination that it can no longer meet its obligations under this Addendum or Data Protection Laws.

3. Data Subject Requests. Vendor shall assist Publix in responding to and implementing Data Subject Requests, including by maintaining appropriate technical and organizational measures to implement or honor such requests.

4. Assessments.

4.1 Vendor will respond promptly to reasonable requests from Publix for information necessary for Publix to assess Vendor's data protection practices, including Vendor's compliance with Data Protection Laws and this DPA.

4.2 Vendor will cooperate with Publix's reasonable efforts to verify Vendor's compliance with this DPA, which efforts may include periodic audits, not to exceed one (1) audit in any twelve (12) month period, except in the event of a Security Incident. Such audit shall be conducted by Publix (or a qualified, independent third party to audit on Publix's behalf) at Publix's expense, unless the results demonstrate Vendor's material non-compliance with its obligations under Data Protection Laws and this DPA, in which case Vendor shall reimburse Publix the reasonable fees spent on such audit. Publix and Vendor shall mutually agree to the dates, times, and scope of any audit of Vendor. The assessments, work papers and other materials generated or used by Publix during the course of the audit shall be treated as Protected Information.

5. Third-Party Demands and Government Access.

5.1 Vendor shall assist Publix in the event of an investigation by any government entity or regulator relating to Publix Personal Data handled by Vendor on Publix's behalf.

5.2 Except as is necessary to fulfil its obligations under any agreement with Publix or as required by law, Vendor shall not disclose any Publix Personal Data to any external party that is not Subprocessor. In the event that Vendor or anyone to whom it transmits the Publix Personal Data becomes legally required to disclose any such Publix Personal Data, Vendor shall provide Publix with prompt written notice so that Publix may seek a protective order or other appropriate remedy. Vendor shall furnish only that portion of the Publix Personal Data that is legally required to be furnished.

6. Security. Vendor shall comply with Publix's requirements and Data Protection Laws regarding the handling, use, storage, security and confidentiality of Protected Information pursuant to Appendix B, Information Security Requirements.

7. General Terms

7.1 Publix shall be entitled to take appropriate action, subject to the provisions of any Agreement, in the event that Vendor misuses Publix Personal Data or otherwise breaches the terms of this DPA, such as suspension of sharing Publix Personal Data or termination of use of Vendor.

7.2 Upon Publix's written or emailed request, but no more than once annually (except in the event of a Security Incident (as defined in Appendix B), to which no such limit shall apply), Vendor shall provide Publix, at no additional cost, with an index describing the Protected Information being held by Vendor. Such report(s) will list each file, table, or other data store of Protected Information. For each listed file, table, or other data store, the report(s) will describe data attributes contained in the listed data set (by way of example, an attribute may be "street address," "customer name," etc.) the number of records, rows, or instances stored, and the creation date for the oldest record, row, or instance stored. The report(s) shall be in a format and medium mutually agreed to by the parties, and shall be provided to Publix no less than thirty (30) calendar days from the date of Publix's request. In addition, Vendor shall provide Publix with a file containing all Protected Information promptly upon Publix's request in a mutually agreed-upon format and at no charge.

7.3 Vendor shall provide a representative within its organization who shall have responsibility to promptly respond to all inquiries of Publix regarding the Processing of Publix Personal Data. Vendor shall provide the contact information for such representative to Publix, and shall immediately notify Publix when the representative changes.

7.4 In the event of any conflict between this DPA and any other agreement between Publix and Vendor, this DPA will control. The obligations of this DPA shall survive for as long as the Vendor holds or Processes Publix Personal Data.

APPENDIX A
PROCESSING INSTRUCTIONS AND DETAILS OF PROCESSING

1. Details of Processing.

1.1 The details regarding Publix Personal Data Processed by Vendors shall be mutually agreed to by the parties.

2. Restrictions on Processing.

2.1 Vendor shall Process Publix Personal Data only as necessary for the provision and enhancement of the Services, which may include:

2.1.1 verifying or maintaining the quality or safety of the Services;

2.1.2 undertaking activities to improve, upgrade, or enhance the Services (or any related features or functionality related thereto);

2.1.3 detecting data security incidents or protecting against malicious, fraudulent, or illegal activity;

2.1.4 complying with Data Protection Laws.

2.2 Vendor shall not:

2.2.1 retain, use, disclose, or otherwise Process Publix Personal Data outside of the direct business relationship between Vendor and Publix or for any commercial purpose other than the purpose of performing the Services specified in the Agreement;

2.2.2 sell or share Publix Personal Data or use Publix Personal Data for targeted advertising;

2.2.3 combine Publix Personal Data with any information that Vendor receives outside the business relationship with Publix.

2.3 Vendor shall ensure that any Authorized User is legally required to keep Publix Personal Data confidential, and that such person will only have access to Publix Personal Data to the extent necessary to perform their job functions.

3. Subprocessing.

3.1 Vendor may not disclose Publix Personal Data to any external party, except that Publix hereby grants general written authorization to Vendor to appoint Subprocessors to perform specific processing activities on its behalf. Where Vendor engages a Subprocessor, Vendor shall:

3.1.1 enter into a written agreement with such Subprocessor that imposes data protection obligations no less protective of Publix Personal Data as those imposed on Vendor under this DPA and that meet the requirements of Data Protection Laws;

3.1.2 perform adequate due diligence regarding the security, privacy and confidentiality practices of each Subprocessor prior to selection and periodically assess each Subprocessor to ensure it is capable of maintaining

the level of protection for Publix Personal Data required by any master agreement, including this DPA;

3.1.3 upon written request from Publix, provide information related to its Subprocessors' data protection and privacy capabilities to Publix within a commercially reasonable timeframe; and

3.1.4 disclose to Subprocessors only the minimum amount of Publix Personal Data necessary to perform the Services.

3.2 Before engaging a new Subprocessor, Vendor will provide written notification to Publix. Publix may object in writing to any additional or replacement Subprocessor on reasonable data protection grounds within ten (10) business days after receipt of any such notice. If Publix objects, Publix and Vendor will discuss commercially reasonable alternatives in good faith.

4. Deletion or Return of Personal Data.

4.1 Vendor shall retain all Protected Information, regardless of medium (i.e., whether in paper, electronic or other form) for a mutually agreed retention period or until such time as Publix approves its destruction and shall follow Publix's instructions with regard to the retention or destruction of such Protected Information. Vendor shall apply industry standard destruction methods (e.g., NIST) to any Protected Information that has been approved by Publix for destruction and shall provide written certification to Publix attesting to its compliance with Publix's instructions promptly thereafter.

4.2 At the termination or expiration date of the Agreement, Vendor shall provide Publix with a copy of any and all remaining Publix Personal Data and then shall delete such Publix Personal Data from Vendor's Information Systems (as defined in Appendix B). Vendor shall promptly certify to Publix that all copies of Publix Personal Data have been deleted in accordance with this requirement.

5. Processing Deidentified Data.

5.1 To the extent Publix discloses or otherwise makes available to Vendor data that has undergone Processing to render it such that it no longer constitutes Personal Data ("Deidentified Data"), Vendor shall (1) adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (2) publicly commit to maintain and use such Deidentified Data in a deidentified form and to not attempt to re-identify the Deidentified Data, except that Vendor may attempt to re-identify the data solely for the purpose of determining whether its deidentification processes are compliant with Privacy Laws; and (3) before sharing Deidentified Data with any other party, including Subprocessors, contractors, or any other persons ("Recipients"), contractually obligate any such Recipients to comply with all requirements of Section 5 of this Appendix A (including imposing this requirement on any further Recipients).

6. Payment Processing and Storage. To the extent that Vendor accepts, transmits or stores cardholder information, the obligations and requirements under this Section shall apply.

6.1 Without limiting the generality of the foregoing, Vendor shall fully comply with the Payment Card Industry ("PCI") Security Standards Council's compliance guidelines, programs and standards, and all other applicable industry standards or regulatory requirements having to do with cardholder information and/or data security, as such

standards or regulations may be modified from time to time. Further, through its acts or omissions, Vendor shall not cause Publix to violate the PCI Security Standards Council's compliance guidelines, programs and standards having to do with cardholder information and/or data security, as such standards may be modified from time to time. Additionally, Vendor shall at all times during the term of the relationship between Publix and Vendor be listed on Visa's Approved Service Provider List. Should Vendor be de-listed from Visa's Approved Service Provider List, Vendor shall promptly notify Publix.

6.2 Vendor shall comply with all industry standard PIN security and key management standards, including but not limited to PCI PIN guidelines as such pertain to Vendor's business relationship with Publix. A specific and detailed written statement of agreed upon exceptions to those sections of the PCI PIN audit (and any future standards) executed by both Publix and Vendor is required for those sections of the PCI PIN audit (or any future industry standard) that Vendor deems not applicable to its business relationship with Publix.

7. Protected Health Information. To the extent that Vendor has access to Protected Health Information (as defined in the Health Insurance Portability and Accountability Act of 1996 as it may be amended or updated from time to time) in connection with the Services provided to Publix, Vendor shall execute and be bound by Publix's Business Associate Agreement ("BA Agreement"). Notwithstanding anything herein to the contrary, in the event of a conflict between the BA Agreement and this DPA, the BA Agreement shall prevail.

APPENDIX B
INFORMATION SECURITY REQUIREMENTS

1. Definitions.

1.1.1 "Information Resources" means all applications, websites, hardware, software, or other computing assets, databases, devices, products, or services used to store, receive, process, access and/or transmit Protected Information and all information technology associated with the creation, collection, processing, use, storage, transmission, analysis and/or disposal of Protected Information.

1.1.2 "PCI PIN" means "PCI PIN Security Standard" published by the PCI Security Standards Council, as such document is amended, replaced and/or updated from time to time.

1.1.3 "Publix Equipment" is any Publix-owned equipment or property.

2. **Reasonable Security**. In addition to and without limiting Vendor's obligations under any Agreement, Vendor shall implement, monitor, and maintain reasonable and appropriate physical, administrative, technical and organizational safeguards appropriately tailored to the nature and scope of its activities and the sensitivity of Protected Information to protect the underlying data which shall in no instance be less protective than the strictest procedures used to secure and retain the confidentiality of its own confidential and proprietary information of a like kind and in all instances will conform to industry standards and any legal requirements and regulatory guidance applicable to such data Processed.

3. **Security Measures**. In order to prevent use of or access to Protected Information by any person other than Authorized Users, Vendor shall implement security measures, including but not limited to:

3.1.1 Vendor shall implement and maintain a written information security policy that specifies the technical and organizational measures it shall apply to safeguard Protected Information in accordance with this DPA. Vendor shall monitor the effectiveness of its written information security policy by conducting periodic self-audits and risk assessments.

3.1.2 Facilities that store Protected Information must implement appropriate controls that restrict both physical and electronic access to Authorized Users only.

3.1.3 Access to Protected Information in any form shall be restricted to Authorized Users with a legitimate need to know such information and who have received appropriate criminal and/or financial background checks, have been properly trained and instructed as to all obligations with respect to the access and use of Protected Information.

3.1.4 Remote access to hardware and/or software that stores, processes or transmits Protected Information must, at a minimum, use multi-factor authentication and generally accepted industry network encryption standards for connection.

3.1.5 Vendor shall implement and maintain secure authentication protocols that

provide for the control of individual user accounts and passwords as set forth below, and controls to ensure that passwords are kept in a location and format that does not compromise the security of the underlying Protected Information.

3.1.6 All Authorized Users must be assigned individual accounts with unique passwords generated or selected using secure methods that are reasonably designed to maintain security of such access control. Default passwords shall not satisfy this requirement.

3.2 The following password requirements must apply to Vendor Information Resources:

3.2.1 Temporary passwords must be given in a secure manner, with expiration on first use;

3.2.2 Passwords must be encrypted or hashed when transmitting over networks and in storage;

3.2.3 Authorized User account credentials must not be shared; and

3.2.4 Strong password practices must be enforced that include minimum password length, lockout, set expiration period, and complexity consistent with relevant industry practices.

3.3 Vendor shall establish and maintain a process to periodically validate that Authorized User accounts with access to Protected Information are necessary to perform the Services. All Authorized User accounts that are no longer required or authorized to access Protected Information, including Publix Information Resources, must be promptly disabled, deleted and removed from all access control lists, security groups, database tables or other methods used to provide the access to Protected Information.

3.4 Vendor shall maintain accurate records sufficient to identify all current and past Authorized Users with access to Protected Information.

3.5 Vendor shall perform network vulnerability scans on Vendor Information Resources at least monthly. Vendor shall perform external penetration testing at least annually. Upon request, Vendor shall provide to Publix formal assessment reports, approved by Vendor's management, of such network vulnerability scans, which shall include at a minimum the scope of the assessment and any vulnerabilities or issues and recommendations. Such formal reports provided by Vendor shall be considered Confidential Information as defined under the Agreement.

3.6 Vendor shall remediate any items rated as critical or high in the assessment report (or similar rating indicating commensurately similar risk) within thirty (30) days of the items being discovered and validated.

3.7 Suspicious or anomalous activity on Vendor Information Resources must be logged and monitored based on Vendor's established procedures, which at a minimum must ensure that the security logs are retained for at least one year and provide an independently verifiable trail sufficient to permit reconstruction, review and examination of the sequence of environments and events surrounding or leading to such suspicious or anomalous activity from inception to termination. Such events shall include but are not limited to: (i) all individual user accesses to Protected Information; (ii) all actions taken by any individual with root or administrative privileges; (iii) invalid logical access attempts; (iv) use of identification and authentication mechanisms; (v)

initialization of audit logs; and (vi) creation and deletion of system-level objects. Audit trails must be secure and unalterable. Upon request, Vendor shall provide Publix with evidence that suspicious or anomalous activity on Vendor Information Resources are logged and monitored.

4. **Encryption**. Vendor shall comply, at a minimum with the following regarding the use of encryption technologies:

4.1.1 Vendor shall use industry best practice encryption technologies and key management practices.

4.1.2 Protected Information must be encrypted at rest and (if applicable) during transmissions over the Internet or other public networks, such as wireless networks, in strict accordance with industry best practices and applicable regulatory standards.

4.2 **System Configuration and Maintenance**. Vendor shall ensure that all Vendor Information Resources comply with each of the following standards:

4.2.1 Vendor shall ensure that all Vendor Information Resources are configured to industry accepted security standards and benchmarks for securely configuring the type of system or device in use.

4.2.2 All Vendor Information Resources, including installed applications, must be patched in accordance with Vendor's established procedures. Additionally, if a patch is identified and evaluated as critical or high by Vendor's established procedures or active exploits exist for vulnerable Vendor Information Resources, the patch must be tested and installed within one month of generally available release to all Vendor Information Resources.

4.2.3 Processes and functionality must be implemented and followed to create accurate and appropriately comprehensive audit trails to identify who has accessed Vendor Information Resources and within any individual applications. Processes must actively monitor and aggregate suspicious or anomalous activity on Vendor Information Resources and Vendor must implement and follow a documented incident response function that is linked to and integrated with the monitoring process.

4.2.4 All Vendor Information Resources must be configured with adequate and up-to-date system security agent software (including malware protection), up-to-date security patches, and up-to-date virus and malware signatures and definitions.

4.2.5 Without express written or email permission from a manager in Publix's IS Security and Compliance group, Protected Information shall not be stored unless it is encrypted: (a) on non-Publix Equipment, including desktops, laptops, tablets, personal digital assistants (PDAs), smart phones or other portable or mobile devices; (b) using removable or movable storage, such as diskettes, compact discs (CDs), DVDs, flash drives or similar devices; or (c) using any third-party Cloud or similar storage service(s).

4.2.6 Any Vendor Information Resources accessed remotely via the Internet, or any extranet must have appropriate security controls implemented to match those stated in this DPA, including, but not limited to, continuous firewalls, up-to-date anti-malware software with current malware

signatures/definitions, current security patches, etc. Vendor shall not store, maintain, transmit, process, allow access to or dispose of Protected Information outside of the continental United States of America without Publix's prior written approval.

4.3 **Network Security**. Vendor shall ensure that all Vendor Information Resources supporting Protected Information comply with each of the following standards:

4.3.1 All Vendor Information Resources must be continuously protected by a firewall to prevent unauthorized access. Only those services and/or protocols needed to support any Vendor Information Resources will be permitted access to such computing devices. All other protocols and services must be denied.

4.3.2 Intrusion detection and/or prevention controls that detect actual or attempted network or computing device compromises must be deployed, properly configured, actively managed, monitored and regularly updated for all Vendor Information Resources and any segments thereof.

4.3.3 Protected Information must not be removed from or transferred to other facilities without the written approval of Publix, except for backup media sent off-site to a storage facility or for electronic replication to alternate data processing facilities previously identified to and approved by Publix.

4.4 **Physical Protections**. Vendor shall ensure that all non-Publix Equipment in or through which Protected Information is accessed, received, stored, maintained, or Processed satisfies each of the following requirements:

4.4.1 Servers, enterprise data storage devices, backup tapes and media, and other hardware and/or software used to store Protected Information must be located in a restricted access location within each facility.

4.4.2 Any facilities, storage areas or containers in which Protected Information is stored shall be locked and access shall be appropriately restricted in accordance with this DPA.

4.4.3 Vendor must have written corporate security policies and procedures that specify physical protection requirements for laptop computers, tablets, PDAs and/or any other portable electronic devices at all times (including while at work and when traveling), which policies and procedures must be documented, regularly communicated to all Vendor employees/agents and enforced.

4.4.4 Vendor shall ensure that all Authorized Users receive periodic training in the proper use of network security and the importance of Protected Information security.

4.4.5 Vendor shall maintain accurate records sufficient to identify all Publix Equipment that stores or accesses Protected Information in the possession of any Authorized Users. Upon request by Publix, or at any time that any such Authorized Users no longer require access to such Publix Equipment (or, if applicable, to access Protected Information), Vendor must promptly collect the Publix Equipment, and confirm and document that such Publix Equipment is appropriately secured and returned to Publix in the manner specified by Publix at the time of notification.

4.5 **Connecting to the Publix Network**.

4.5.1 Any Vendor Information Resources that may connect to Publix Information Resources must comply with all applicable provisions of this DPA.

4.5.2 Any Authorized User that requires connection to the Publix network in order to perform the Services must be setup within Publix's third-party connectivity solution to facilitate a security connection and must comply with all applicable provisions of this DPA.

4.5.3 Vendor shall promptly notify Publix should a (i) Vendor Information Resource, (ii) Authorized User, or (iii) electronic business connection (e.g., VPN, Dial Up, SSH, etc.) no longer be required or authorized to obtain access to Publix Information Resources. Publix retains the right to deny or disable access to Publix Information Resources to some or all Vendor employees, agents, or Subprocessors at Publix's sole discretion.

4.6 **Security Incidents**.

4.6.1 Vendor shall maintain a process for managing suspected or actual Security Incidents. "Security Incident" means the actual occurrence or the substantial likelihood of the occurrence of one or more of the following: (i) loss, misuse, unauthorized access, acquisition, or use of Protected Information, (ii) unauthorized access to Publix Information Resources or Vendor Information Resources, (iii) an impact to the confidentiality, integrity, or availability of Protected Information, Publix Information Resources, or Vendor Information Resources), or (iv) malware posing a significant threat to such information or Services (including, without limitation, ransomware).

4.6.2 Subject to the terms of any Agreement between the Parties, Vendor shall, at its sole cost and expense, promptly (and in any event within forty-eight (48) hours) notify Publix of any Security Incident or any other breach of the protection of Protected Information or failure in the safeguards protecting such information, regardless of whether Data Protection Laws require reports to regulators or notification to individuals. Publix is solely responsible for determining whether to notify impacted Data Subjects and for determining whether relevant supervisory authorities need to be notified of a Security Incident as may be required solely for Publix's own business and activities, however nothing in this Section will impose any notification obligations on Publix with regard to Vendor's business and activities.

4.6.3 Upon discovery of a Security Incident, Vendor shall take immediate action including, but not limited to, engaging a forensic investigator as appropriate, at its own expense and in compliance with applicable law, to: (i) investigate the Security Incident; (ii) identify, prevent and mitigate the effects of the Security Incident; (iii) perform all actions (including but not limited to implementing those remedial measures proposed by the forensic investigator, if any) reasonably necessary to remedy the Security Incident, prevent future incidents of the same or similar nature, and to otherwise restore the confidentiality, security and integrity of the Protected Information; and (iv) perform those actions and provide the support requested by Publix. Vendor shall pay for or reimburse Publix for all damages, costs, losses, and expenses related to a Security Incident, including, but not limited to, all damages, costs, losses and expenses

incurred by Publix in preparing and providing notice to impacted persons and the media pursuant to applicable law, as well as other related support services such as credit monitoring services and call center services.

4.6.4 The Security Incident notification shall be sent via electronic mail to the following Publix representative, as may be modified by Publix from time to time (the "Security Incident Contact"):

Publix's Computer Incident Response Team (CIRT)
E-mail: cirt@publix.com
Telephone: 1-866-994-CIRT

In addition to notifying Publix via electronic email, Vendor shall notify the same Security Incident Contact by either (i) contacting the Security Incident Contact via telephone, or (ii) through such other contact method as reasonably required by Publix.

4.6.5 The Security Incident notification shall include, to the extent such information is available to Vendor: (i) a detailed description of such Security Incident; (ii) the specific Protected Information impacted; (iii) the identity of each affected person; (iv) measures taken by Vendor to identify, prevent and mitigate the effects of the Security Incident; and (v) any other relevant information and documentation that Publix may request concerning the Security Incident. Vendor shall not delay notification because of insufficient information but rather shall provide and supplement notifications as information becomes available. Vendor shall provide Publix with written updates to the Security Incident notification on a daily basis (or at a different interval agreed by Publix) until the Security Incident has been resolved to Publix's satisfaction.

4.6.6 Vendor shall not disclose (or permit any third party to disclose) the occurrence of, or any information relating to, a Security Incident or make any notification to regulatory authorities or Data Subjects without Publix's explicit written authorization, except as required by applicable law.

4.7 **Security Audits.**

4.7.1 At least annually and upon request and at no additional cost to Publix, Vendor will undergo a SSAE SOC 1 and/or 2 Type II Audit Report or latest industry equivalent and shall provide Publix with an update of such report or latest industry equivalent on an annual basis upon request during the term of the Agreement.

4.7.2 Vendor shall provide Publix, within thirty (30) calendar days from the date of Publix's request and at no additional cost, with copies of all relevant audits and/or assessment reports that Vendor has obtained for its operations, including but not limited to the following: PCI security standards assessments (including PTS, PA-DSS, P2P Encryption and DSS), PCI PIN audits, financial audits and reports, internal control audits, and security and business resumption testing. In the event that the foregoing audits or assessment reports do not provide detail reasonably sufficient to Publix, as determined solely by Publix, Vendor shall obtain within thirty (30) days from the date of Publix's request, at its own cost and expense, such additional audits and/or assessment reports as requested by Publix.

4.8 **Business Resumption and Contingency**. Vendor shall maintain and comply with a business resumption and contingency plan for its operations and the processing and storage of all Protected Information to ensure that all Protected Information and Vendor's operations and data will be available to the maximum extent possible including, but not limited to, immutable backups of Protected Information to mitigate the risk of ransomware attacks and to avoid loss of such Protected Information in the event of an attack. All immutable backups shall allow for the recovery, restoration and access to any and all Protected Information.