EXHIBIT B

Confidential Information and Data Processing Addendum

This Confidential Information and Data Processing Addendum (this "**DPA**") is attached and made part of the Software Services Agreement (the **"Agreement**") between Seminole County (the "County") and the Contractor (collectively, "Parties," individually, "Party"), which collects, transmits, uses, maintains, or processes Personal Information (as defined in Section 1.2, below) on behalf of the County pursuant to the Agreement (as identified in the Agreement, including the Scope of Services).

1. General

1.1. Capitalized terms used but not defined in this DPA will have the meanings assigned to them in the Agreement and, if not defined in either this DPA nor the Agreement, shall have the ordinary meaning in the field of information technology services.

1.2. Contractor may process and/or receive "personal information" or "personal data" from, or on behalf of, the County. "Personal Information" or "Personal Data" shall be defined as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household (herein referred to as "Personal Information"). For avoidance of doubt, Personal Information shall include the definition as used in § 501.171, F.S., Protected Health Information as defined in 45 C.F.R. § 160.103, Nonpublic Personal Information as defined in 15 U.S.C. § 6809(4)(A), and credit card data as used in the Payment Card Industry Data Security Standard ("PCI DSS").

1.3. In connection with providing services to the County, the County and Contractor may each share Confidential Information with the other Party. With respect to the County, "Confidential Information" means all data, information, and material provided by, or received from, the County that is statutorily exempt from applicable public records laws. For avoidance of doubt, all Personal Information will be deemed and treated as the County's Confidential Information. With respect to Contractor, "Confidential Information" means those documents and materials provided by Contractor that (i) qualify as Trade Secrets (as defined in Sections, 119.0715(2) and 688.022, F.S.), and (ii) are clearly labeled or marked as "TRADE SECRET" or "CONFIDENTIAL" upon delivery to the County. Vendor understands and agrees that it must label all Trade Secrets in writing upon delivery to the County to invoke exemptions from applicable public records laws.

1.4. The Contractor to this DPA agrees that Contractor will treat as confidential all information provided by, or collected on behalf of, the County, including, without limitation, unencrypted Personal Information and non-public information to the extent authorized by Florida Statutes.

1.5. Notices required under this DPA shall be sent according to the Services Agreement with a copy (which shall not constitute notice) to both the usual point of contact or support at the County and via email to: **purch@seminolecountyfl.gov** with the subject line as: "Data Processing Addendum Notice."

1.6. The Contractor shall carry out the services and process Personal Information received from, or collected on behalf of, the County as set out in the Agreement or as otherwise notified in writing by the County to the Contractor during the term of the Agreement.

2. Observance of Laws, Regulations, and Standards

2.1. The Contractor, when applicable, will ensure that the data designated for collection, transfer, or processing as part of agreed upon services will be collected, transferred, and processed in a fully compliant manner to enable the County to meet relevant requirements of all laws, regulations, and contractual requirements applicable to the County, including, but not limited to, the current versions of:

2.1.1. Personal Identifiable Information

2.1.1.1. Florida Information Protection Act (F.S. 501.171);

2.1.1.2. Any other similar laws currently in effect or that may come into effect during the term of the Agreement, including the laws of states other than Florida, to the extent Contractor collects or processes Personal Information of residents of other states in connection with the Agreement;

3. Permitted Uses and Disclosures

3.1. Personal Information

3.1.1. Contractor shall use, disclose, and retain all Personal Information:

3.1.1.1. As specifically authorized in the Agreement and this DPA;

3.1.1.2. Solely for the purpose of performing the services described in the Agreement; and

3.1.1.3. In accordance with applicable laws, standards and regulations.

3.1.2. Contractor shall not sell, rent, transfer, distribute, or otherwise disclose or make available any Personal Information to any third party without prior written permission from the County, unless and to the extent required by law. To the extent written authorization is provided by County, Contractor may disclose Personal Information to such third

parties, provided that such third parties are subject to written data processing addenda that are consistent with, and at least as protective of the Personal Information as, this DPA. Contractor understands that under no circumstance will it, or any third parties, process Personal Information outside of the United States. Notwithstanding the foregoing, Subject to Section 12 ("Subcontractors") of the Agreement, Contractor is authorized by the County to use third parties, as well as employees and contractors of Contractor's affiliates and subsidiaries, in performance of its obligations described in the Agreement.

3.1.3. Contractor shall:

3.1.3.1. Promptly notify the County of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking Personal Information provided by, or collected on behalf of, the County;

3.1.3.2. Consult with the County regarding its response;

3.1.3.3. Cooperate with the County's reasonable requests in connection with efforts by the County to intervene and quash or modify the legal order, demand or request; and

3.1.3.4. Upon the County's request, provide the County with a copy of its response.

3.2. Other Confidential Information

3.2.1. Contractor shall treat all County Confidential Information as strictly confidential and (i) shall not use such information for any purpose other than providing services to and for the benefit of the County as required under the Agreement, (ii) shall not (absent written consent from the County) disclose any County Confidential Information to any person or entity other than an employee or contractor of the Contractor who is authorized by County in writing (provided that all such contractors are subject to written confidentiality obligations at least as protective of those set forth in this DPA) that has a need to know such Confidential Information to perform its obligations under the Agreement, (iii) take all appropriate and commercially reasonable steps to protect such Confidential Information, and (iv) promptly notify the County in writing in the event of any actual unauthorized disclosure or use of County Confidential Information.

3.2.2. The obligations for protection, non-use and non-disclosure of County Confidential Information hereunder must last during the term of the Agreement and for so long thereafter as the applicable County Confidential Information is not subject to disclosure under statutory public records laws.

3.2.3. Contractor understands and agrees that Confidential Information received from the County must be treated as Confidential Information subject to the protection of this Section 3.2, regardless of whether or not similar or equivalent information may be obtainable from other sources. The County understands and agrees that information and material properly independently developed or legally obtained from third party sources, in each case without use of or reference to County Confidential Information, shall not be considered County Confidential Information pursuant to this Section 3.2.

3.3. All Personal Information shall be deemed and treated as Confidential Information and shall be protected, processed, stored and otherwise handled (i) as Confidential Information, and (ii) as required by applicable laws.

3.4. If the County receives a subpoena, warrant, public records request pursuant to Chapter 119, F.S., or other legal order, demand or request seeking Confidential Information (including without limitation Personal Information) provided by, or on behalf of, the County and maintained by Contractor, the County will notify Contractor of such request. Upon such notice, Contractor shall promptly supply the County with copies of materials and data required for the County to respond. Contractor shall further cooperate with the County's reasonable requests in connection with its response. Should the County receive any subpoena, warrant, or other legal order, demand or request seeking Contractor Confidential Information, the County shall promptly notify Contractor of such request and shall cooperate with Contractor's reasonable requests in connection with its response provided, however, that at all times the County shall comply with all applicable laws and orders in its sole discretion.

3.5. Under no circumstances will Contractor disclose or use any Personal Information, including Protected Health Information, Financial Information, and Credit Card Data, or other Confidential Information for any purposes whatsoever other than (i) to provide services to the County subject to the Agreement, or (ii) as otherwise required by law after providing all reasonable notice to the County, both during and after the term of the Agreement.

4. Data Security Obligations.

4.1. Contractor shall:

4.1.1. Implement a comprehensive information security program which includes generally accepted best practices for industry cybersecurity, as defined in F. S. § 282.3185, and technical and administrative safeguards to protect the confidentiality of Personal Information that are no less rigorous than commercial best practices for information security;

4.1.2. Keep all Personal Information contained in any format (e.g., paper, computer system, and removable media) in a secure facility where access of unauthorized personnel is restricted;

4.1.3. Ensure that all Personal Information received from, or collected on behalf of, the County remains in the continental United States at all times;

4.1.4. Install up-to-date firewall protection and operating system patches for files containing Personal Information on a

system that is connected to any network;

4.1.5. Install up-to-date versions of system security agent software which includes malware protection and reasonably up-to-date 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, on systems vulnerable to malware and containing or channeling access to systems containing Personal Information;

4.1.6. Implement secure user authentication protocols including:

4.1.6.1. Control of user IDs and other identifiers;

4.1.6.2. A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as token devices;

4.1.6.3. 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;

4.1.6.4. Restricting access to active users and active user accounts only; and

4.1.6.5. Blocking access to user identification after multiple unsuccessful attempts to gain access or exceeding the limitation placed on access for the particular system;

4.1.7. Implement secure access control measures that:

4.1.7.1. Restrict access to records and files containing Personal Information to those who need such information to perform their job's duties; and

4.1.7.2. Assign unique identifications plus passwords, which are not Contractor supplied default passwords, to each person with computer access that are reasonably designed to maintain the integrity of the security of the access controls;

4.1.8. Use strong encryption in the following situations:

4.1.8.1. When Personal Information is transmitted over a public network;

4.1.8.2. When Personal Information is stored in non-removable media prior to, or after, processing; and

4.1.8.3. When Personal Information is stored on removable media and that media is in transit between physical locations;

4.1.9. Provide ongoing employee training with respect to its information security program, the proper use of the computer security system, and the importance of Personal Information security;

4.1.10. Ensure that any employee or contractor of the Contractor who has access to Personal Information resides, and accesses such Personal Information while, in the continental United States;

4.1.11. Designate responsibility for maintaining Contractor's comprehensive information security program;

4.1.12. Oversee its third-party service providers by taking reasonable steps to select and retain third-party service providers that are capable of maintaining security measures to protect Personal Information consistent with the Agreement, including the Scope of Services, this DPA, and applicable laws;

4.1.13. Review the scope of its comprehensive security program at least once a year for the term of the Agreement; and

4.1.14. Document responsive actions taken in connection with any incident involving a Security or Privacy Breach, and mandatory post-incident reviews of events and actions taken, if any, in order to make changes in business practices relating to the protection of Personal Information, and promptly provide such documentation to County.

4.1.15. Maintain plans for business continuity, disaster recovery, and backup capabilities and facilities designed to ensure the Contractor's continued performance of its obligations under the Agreement, including, without limitation, loss of production, loss of systems, loss of equipment, failure of carriers and the failure of the Contractor's or its supplier's equipment, computer systems or business systems ("Business Continuity Plan"). Such Business Continuity Plan shall include, but shall not be limited to, testing, accountability, and corrective actions designed to be promptly implemented, if necessary. Contractor represents that, as of the date of this DPA, such Business Continuity Plan is active and functioning normally in all material respects. Contractor shall perform a comprehensive test of its Business Continuity Plan no less than once per calendar year. Contractor further represents that, all parties that are storing or processing unencrypted Personal Information, as part of the Business Continuity Plan or otherwise, must agree to and abide by this DPA.

5. Additional Rights and Obligations

5.1. Contractor, at its own expense, shall arrange for a qualified and independent assessor, using an appropriate and accepted control standard or framework and assessment procedure, to conduct a review, scan, assessment, audit, or other policy review and testing of Contractor's policies and technical and organizational measures to satisfy its obligations under this DPA. Contractor shall provide a report of all such review, scan, assessment, audit, or test to the County upon request.

5.2. To the extent Contractor obtains any audit report or similar assessment regarding its operations or any system or data relating to the Personal Information, Contractor shall make such report or assessment available to the County upon written request and at no charge. To the extent such report or assessment determines that Contractor's processes, systems, networks or operations have a material deviation from the applicable standard or best practices, (i) Contractor shall promptly provide all reasonably requested information relating to the deviation that may be requested by the County, (ii) Contractor shall promptly provide a reasonably detailed remediation plan to the County and provide regular updates on the completion of such plan, and (iii) the County shall have the right to suspend or terminate Contractor's processing of Personal Information without charge or penalty until such deviation has been corrected, or to terminate the Agreement with no charge or penalty in the event such deviation is not timely corrected.

6. Security or Privacy Breach

6.1. For purposes of this DPA, the term, "Breach of Security" or "Breach" has the meaning given to it under the applicable Florida Statute (F.S. 501.171(1)(a)), applicable state or federal rule/regulation, or contractual obligation.

6.2. Upon becoming aware of a Breach of Security or Breach, or of circumstances that could have resulted in unauthorized access to or disclosure or use of Personal Information, Contractor shall notify the County in the most expedient time possible and without unreasonable delay, fully investigate the incident, and reasonably cooperate with the County's investigation of and response to the incident. Except as otherwise required by law, Contractor will not provide notice of the incident directly to individuals whose Personal Information was involved, regulatory agencies, or other entities, without prior written permission from the County.

6.3. The report provided under section 6.2 of this DPA shall identify:

6.3.1. The nature of the unauthorized access, use, or disclosure;

6.3.2. The Personal Information accessed, used, or disclosed;

6.3.3. The person(s) or entities who accessed, used, and disclosed and/or received Personal Information (if known);

6.3.4. What Contractor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure;

6.3.5. What corrective action Contractor has taken or will take to prevent future unauthorized access, use or disclosure;

6.3.6. Contractor shall provide such other information, including a written report, as reasonably requested by the County.

6.4. In the event of any Breach of Security or Breach, the County shall have the right to suspend or terminate Contractor's processing of Personal Information without charge or penalty until such breach has been corrected, or to terminate the Agreement with no charge or penalty in the event Contractor does not timely correct the cause of the breach, reasonably cooperate with the County in any remediation effort, and take such other corrective actions as the County may reasonably require, all in a timely fashion.

6.5. Under no circumstances will Contractor make any public statement regarding any Breach of Security or Breach that relates to any Personal Information without the prior written consent of the County, such consent not to be unreasonably withheld, conditioned or delayed.

7. Other Obligations of Contractor

7.1. Vendor shall defend, indemnify and hold the County harmless from and against any and all third party liabilities, losses, damages and costs, including reasonable attorneys' fees (collectively, "Losses"), to the extent resulting from Contractor's breach of its duties or obligations under this DPA.

8. Obligations of the County

8.1. The County is solely responsible for:

8.1.1. Ensuring that any consents required by law and/or the County policies and procedures for the collection, access, use, maintenance, and/or disclosure of the Personal Information have been obtained from each individual and entity (including, without limitation, consumers, business Clients, and/or the County's employees and contractors) to whom the Personal Information relates;

8.1.2. Rendering any Personal Information on its systems unusable, unreadable, or indecipherable to unauthorized individuals in accordance with industry standards. The County acknowledges that it is the County's responsibility to encrypt all data on the County's systems and media components prior to providing such Personal Information to Contractor for any reason;

8.1.3. Establishing the applicable information security safeguards and associated policies for protecting Personal Information in its facilities; and

8.1.4. Promptly informing the Contractor of any policies that it implements with respect to the processing and protection of Personal Information with express instructions as to how these policies should be implemented by the Contractor.

9. Miscellaneous

9.1. Any ambiguity in the terms of this DPA will be resolved to permit Contractor or the County to comply with applicable laws.

9.2. To the extent there are any inconsistencies between the terms of this DPA and the terms of the Agreement, this DPA will prevail.