AGREEMENT

THIS AGREEMENT is made and entered into as of this ____ day of _____, _____, by and between

THE SCHOOL BOARD OF BROWARD COUNTY, FLORIDA
(Hereinafter referred to as "SBBC"),
a body corporate and political subdivision of the State of Florida,
whose principal place of business is
600 Southeast Third Avenue
Fort Lauderdale, Florida 33301

and

Performance Matters LLC
(Hereinafter referred to as "VENDOR"),
whose principal place of business is
7730 Union Park Ave, Suite 500
Sandy, UT 84047

WHEREAS, SBBC issued a Request for Proposal identified as RFP 18-097E, Professional Development Management Software System and Services (hereinafter referred to as "RFP"), dated August 22, 2017, and amended by Addendum No. 1 dated September 6, 2017, Addendum No. 2 dated September 6, 2017, Addendum No. 3 dated September 14, 2017 and Addendum No. 4 dated September 20, 2017, each of which is incorporated by reference herein, for the purpose of receiving proposals for Professional Development Management Software System and Services; and

WHEREAS, VENDOR offered a proposal in response to the RFP (hereinafter referred to as "Proposal") and which is incorporated herein by reference whereby VENDOR proposed to provide a professional development management software system (PDMS) to manage, track and report professional development via a comprehensive single sign-on system. This entails searching, cataloging, reporting, registration, documentation and compliance participation for approximately 50,000 internal (certified and non-certified) and external users; and

WHEREAS, VENDOR shall provide a fully developed, readily available, fully functional system, per SBBC requirements, no later than the last week of June 2018; and

WHEREAS, SBBC desires to purchase goods and services from the VENDOR; and

WHEREAS, the SBBC and VENDOR desire to memorialize the terms and conditions of their agreement.

NOW, THEREFORE, in consideration of the premises and of the mutual covenants contained herein and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

ARTICLE 1 – RECITALS

1.0 **Recitals.** The parties agree that the foregoing recitals are true and correct and that such recitals are incorporated herein by reference.

ARTICLE 2 – SPECIAL CONDITIONS

2.0 **Term of Agreement.** Unless terminated earlier pursuant to Section 3.06 of this Agreement, the term of this Agreement shall commence upon execution of both parties and conclude on **June 30, 2021.** The term of the contract may, by mutual agreement between SBBC and VENDOR, be extended for two additional one-year periods and, if needed, 180 days beyond the expiration date of the renewal period.

2.01 **Priority Documents:** In the event of a conflict between documents, the following priority of documents shall govern.

First:	This Agreement; then
Second:	Addendum No. 4 to RFP 18-097E; then
Third:	Addendum No. 3 to RFP 18-097E; then
Third:	Addendum No. 2 to RFP 18-097E; then
Fourth:	Addendum No. 1 to RFP 18-097E; then
Fifth:	RFP 18-097E - Professional Development Management Software System and Services; then
Sixth:	Proposal submitted by VENDOR in response to RFP 18-097E.

2.02 **Cost of Services.** SBBC shall pay VENDOR for services rendered under this Agreement based on prices included in their proposal, within thirty (30) days of receipt of an invoice from the VENDOR, see **Attachment A**. Payment shall be made upon delivery of a fully developed, readily available, fully functional system, per SBBC requirements.

The District's preferred method of payment is via ACH electronic payments. An electronic payment can reduce processing time and administrative overhead costs for both parties, resulting in expedited payment upon invoice approval, and reduces exposure to check fraud. SBBC will not pay convenience fees, surcharges, or any additional costs for payments made by electronic payment.

2.03 **Subsequent Purchases**. Any updates, revisions, enhancements or changes in scope, products, or price that are requested by SBBC and not provided for in VENDOR's Proposal of this Agreement, must be documented in a Service Change Request ("SCR"), see **Attachment B** and an Amendment to this Agreement. Each SCR must be executed by both parties prior to VENDOR commencing any of the work requested.

2.04 **Scope of Services.** VENDOR shall provide SBBC with the products and services specified in their Proposal which includes but is not limited to:

a) Design and implementation of an external user registration process, including all integrations at no additional charge to SBBC.

b) The integration with CyberSource, the e-commerce service provider currently used by SBBC, is included at no additional charge to SBBC (third party product integration).

c) The following environments shall be maintained during the tenure of the Agreement for testing and training purposes at no additional charge to SBBC.
   1. User Acceptance Testing (UAT)
   2. Production

   The environments shall be maintained in perpetuity on behalf of SBBC.

d) Data migration of all in-service records for all users from the system of record, SAP.

e) VENDOR and SBBC shall collaborate to develop a training plan, including all training materials that meets the requirements of SBBC. Training shall be conducted in an SBBC environment.

f) VENDOR shall collaborate with SBBC to create an implementation plan that consists of project monitoring, clear and measurable milestones, a well-defined path for issue resolution and change control.

2.05 **Employee and Non-Employee Information.**

i. SBBC will disclose or provide access to **employee** information to VENDOR for the following purposes:

   a) to build user profiles from data stored in SAP, the District's system of record. Information to be disclosed includes personnel number, first and last name, date of birth, employee status, employment date, organizational assigment, position type, job classification, email address, mailing address, degrees/education, certifications, qualifications, building and location assigment, historical inservice records.

   b) to recommend available professional development based on personnel evaluation scores. Information to be disclosed includes personnel number, first and last name, final evaluation score, instructional practice score, deliberate practice score, VAM score (provided by the State) and individual element scoring.

   c) to ensure accurate state reporting and certification processing, awardees shall provide all completed in-service records for all users back to SAP. Information to be disclosed includes personnel number, course identification number, number and type of points awarded, course dates and completion dates.

ii. SBBC will store **non-employee** information as follows:

   a. to create "non-employee" user accounts, and to reactivate or create a profile in SAP. Information to be storedin SAP includes first and last name, social security number, date of birth, user type, school location (if applicable), position, email address, mailing address, phone number, gender, ethnic origin, race and certifications.

b. Social security number, gender, ethnic origin and race are not stored in the VENDOR's system. This information is collected and used to create a profile in SAP, however the VENDOR will not have access or see this information. This information would then be stored in SAP only.

iii. SBBC shall pass through employee and non-employee information to the VENDOR without disclosing confidential personally identifiable information (i.e., social security number, gender, race and ethnic origin).

"Non-employees" are charter school employees, other Florida School District employees, retirees, or anyone not employed by SBBC who registers to participate in our professional development offerings. SBBC shall not disclose or provide access to information from education records (k-12) to VENDOR.

2.06 **Safeguarding confidential records.** Notwithstanding any provision to the contrary within this Agreement, VENDOR shall 1) fully comply with the requirements of state or federal law or regulation regarding the confidentiality of employee and non-employee records, 2) hold the records in strict confidence and not use or disclose same except as required by this Agreement or as required or permitted by law, 3) only share records with those who have a need to access the information in order to perform their assigned duties in the performance of this Agreement, 4) protect the records through administrative, physical and technological safeguards to ensure adequate controls are in place to protect the records, 5) notify SBBC immediately upon discovery of a breach of confidentiality of the records by telephone and email at 754-321-0300 (Manager, Information Security) and 754-321-1900 (Privacy Officer), privacy@browardschools.com; and take all necessary notification steps as may be required by federal and Florida law, including, but not limited to, those required by Section 501.171, Florida Statutes, 6) prepare and distribute, at its own cost, any and all required notifications, under federal and Florida Law, or reimburse SBBC any direct costs incurred by SBBC for doing so, and 7) be responsible for any fines or penalties for failure to meet notice requirements pursuant to federal and/or Florida law. This section shall survive the termination of all performance or obligations under this Agreement.

2.07 **Inspection of VENDOR Records by SBBC:** VENDOR shall establish and maintain books, records and documents (including electronic storage media) sufficient to reflect all income and expenditures of funds provided by SBBC under this Agreement. All VENDOR Records, regardless of the form in which they are kept, shall be open to inspection and subject to audit, inspection, examination, evaluation and/or reproduction, during normal working hours, by SBBC's agent or its authorized representative to permit SBBC to evaluate, analyze and verify the satisfactory performance of the terms and conditions of this Agreement and to evaluate, analyze and verify any and all invoices, billings, payments and/or claims submitted by VENDOR or any of VENDOR'S payees pursuant to this Agreement. VENDOR Records subject to examination shall include, without limitation, those records necessary to evaluate and verify direct and indirect costs (including overhead allocations) as they may apply to costs associated with this Agreement. VENDOR Records subject to this section shall include any and all documents pertinent to the evaluation, analysis, verification and reconciliation of any and all expenditures under this Agreement without regard to funding sources.

(a) VENDOR Records Defined. For the purposes of this Agreement, the term "VENDOR Records" shall include, without limitation, accounting records, payroll time sheets, cancelled payroll checks, W-2 forms, written policies and procedures, computer records, disks and software,

videos, photographs, executed subcontracts, subcontract files (including proposals of successful and unsuccessful bidders), original estimates, estimating worksheets, correspondence, change order files (including sufficient supporting documentation and documentation covering negotiated settlements), and any other supporting documents that would substantiate, reconcile or refute any charges and/or expenditures related to this Agreement.

(b) Duration of Right to Inspect. For the purpose of such audits, inspections, examinations, evaluations and/or reproductions, SBBC's agent or authorized representative shall have access to VENDOR Records from the effective date of this Agreement, for the duration of the term of this Agreement, and until the later of five (5) years after the termination of this Agreement or five (5) years after the date of final payment by SBBC to VENDOR pursuant to this Agreement.

(c) Notice of Inspection. SBBC's agent or its authorized representative shall provide VENDOR reasonable advance notice (not to exceed two (2) weeks) of any intended audit, inspection, examination, evaluation and or reproduction.

(d) Audit Site Conditions. SBBC's agent or its authorized representative shall have access to the VENDOR'S facilities and to any and all records related to this Agreement, and shall be provided adequate and appropriate work space in order to exercise the rights permitted under this section.

(e) Failure to Permit Inspection. Failure by VENDOR to permit audit, inspection, examination, evaluation and/or reproduction as permitted under this Section shall constitute grounds for termination of this Agreement by SBBC for cause and shall be grounds for the denial of some or all of any VENDOR claims for payment by SBBC.

(f) Overcharges and Unauthorized Charges. If an audit conducted in accordance with this Section discloses overcharges or unauthorized charges to SBBC by VENDOR in excess of two percent (2%) of the total billings under this Agreement, the actual cost of SBBC's audit shall be paid by the VENDOR. If the audit discloses billings or charges to which the VENDOR is not contractually entitled, the VENDOR shall pay said sum to SBBC within twenty (20) days of receipt of written demand under otherwise agreed to in writing by both parties.

(g) Inspection of Subcontractor's Records. VENDOR shall require any and all subcontractors, insurance agents and material suppliers (hereafter referred to as "Payees") providing services or goods with regard to this Agreement to comply with the requirements of this section by insertion of such requirements in any written subcontract. Failure by VENDOR to include such requirements in any subcontract shall constitute grounds for termination of this Agreement by SBBC for cause and shall be grounds for the exclusion of some or all of any Payee's costs from amounts payable by SBBC to VENDOR pursuant to this Agreement and such excluded costs shall become the liability of the VENDOR.

(h) Inspector General Audits. VENDOR shall comply and cooperate immediately with any inspections, reviews, investigations, or audits deemed necessary by the Florida Office of the Inspector General or by any other state or federal officials.

2.08 **Information Security Guidelines**. VENDOR shall follow all associated Information and Technology security requirements, see **Attachment C**.

2.09 **Notice:** When any of the parties desire to give notice to the other, such notice must be in writing, sent by U.S. Mail, postage prepaid, addressed to the party for whom it is intended at the place last specified; the place for giving notice shall remain such until it is changed by written notice in compliance with the provisions of this paragraph. For the present, the Parties designate the following as the respective places for giving notice:

To SBBC:	Superintendent of Schools The School Board of Broward County, Florida 600 Southeast Third Avenue Fort Lauderdale, Florida 33301
With a Copy to:	Chief Academic Officer The School Board of Broward County, Florida 3531 Davie Road Davie, Florida 33314
To VENDOR:	Adam Klaber; Chief Executive Officer **Performance Matters LLC** 7730 Union Park Blvd.; Suite 500 Sandy, UT 84047
With a Copy to:	James H, Curtin, Director of Legal Affairs **Performance Matters LLC** 8860 E. Chaparral Rd, Ste. 100 Scottsdale, AZ 85251

2.10 **BACKGROUND SCREENING.** VENDOR agrees to comply with all requirements of Sections 1012.32 and 1012.465, Florida Statutes, and all of its personnel who (1) are to be permitted access to school grounds when students are present, (2) will have direct contact with students, or (3) have access or control of school funds, will successfully complete the background screening required by the referenced statutes and meet the standards established by the statutes. This background screening will be conducted by SBBC in advance of the VENDOR or its personnel providing any services under the conditions described in the previous sentence. VENDOR shall bear the cost of acquiring the background screening required by Section 1012.32, Florida Statutes, and any fee imposed by the Florida Department of Law Enforcement to maintain the fingerprints provided with respect to the VENDOR and its personnel. The parties agree that the failure of VENDOR to perform any of the duties described in this section shall constitute a material breach of this Agreement entitling SBBC to terminate immediately with no further responsibilities or duties to perform under this Agreement. VENDOR agrees to indemnify and hold harmless SBBC, its officers and employees from any liability in the form of physical or mental injury, death or property damage resulting from VENDOR'S failure to comply with the requirements of this Section or with Sections 1012.32 and 1012.465, Florida Statutes.

2.11 **Insurance Requirements.** Vendor shall comply with the following insurance requirements throughout the term of this Agreement.

(a) General Liability. Limits not less than $1,000,000 per occurrence for Bodily Injury/ Property Damage; $1,000,000 General Aggregate. Limits not less than $1,000,000 for Products/Completed Operations Aggregate.

(b) Professional Liability/Errors & Omissions. Limit not less than $1,000,000 per occurrence covering services provided under this Agreement.

(c) Workers' Compensation. Florida Statutory limits in accordance with Chapter 440; Employer's Liability limits not less than $100,000/$100,000/$500,000 (each accident/disease-each employee/disease-policy limit)..

(d) Auto Liability. Owned, Non-Owned and Hired Auto Liability with Bodily Injury and Property Damage limits of not less than $1,000,000 Combined Single Limit.

If Awardee does not own any vehicles, hired and non-owned automobile liability coverage in the amount of $1,000,000 shall be accepted. In addition, an affidavit signed by the Awardee must be furnished to SBBC indicating the following:

_____ (Awardee Name) does not own any vehicles. In the event insured acquires any vehicles throughout the term of this agreement, insured agrees to provide proof of "Any Auto" coverage effective the date of acquisition..

(e) Acceptability of Insurance Carriers. The insurance policies shall be issued by companies qualified to do business in the State of Florida. The insurance companies must be rated at least A- VI by AM Best or Aa3 by Moody's Investor Service.

(f) Verification of Coverage. Proof of Insurance must be furnished within 15 days of execution of this Agreement. To streamline this process, SBBC has partnered with EXIGIS RiskWorks to collect and verify insurance documentation. All certificates (and any required documents) must be received and approved by SBBC before any work commences to permit Awardee time to remedy any deficiencies. EXIGIS RiskWorks will send an email notification within three (3) business days after receipt of the award letter.

- New vendors will receive an email notification requesting account verification and insurance agent information.
- Existing vendors will receive an email notification of current status.

(g) Required Conditions. Liability policies must contain the following provisions. In addition, the following wording must be included on the Certificate of Insurance:

1. The School Board of Broward County, Florida, its members, officers, employees and agents are added as additional insured.

2. All liability policies are primary of all other valid and collectable coverage maintained by the School Board of Broward County, Florida.

3. Certificate Holder: The School Board of Broward County, Florida, c/o EXIGIS Risk Management Services, P. O. Box 4668-ECM, New York, New York 10163-4668

(h) Cancellation of Insurance. Vendors are prohibited from providing services under this Agreement with SBBC without the minimum required insurance coverage and must notify SBBC within two business days if required insurance is cancelled.

The School Board of Broward County, Florida reserves the right to review, reject or accept any required policies of insurance, including limits, coverages or endorsements, herein throughout the term of this agreement.

ARTICLE 3 – GENERAL CONDITIONS

3.01 **No Waiver of Sovereign Immunity.** Nothing herein is intended to serve as a waiver of sovereign immunity by any agency or political subdivision to which sovereign immunity may be applicable or of any rights or limits to liability existing under Section 768.28, Florida Statutes. This section shall survive the termination of all performance or obligations under this Agreement and shall be fully binding until such time as any proceeding brought on account of this Agreement is barred by any applicable statute of limitations.

3.02 **No Third Party Beneficiaries.** The parties expressly acknowledge that it is not their intent to create or confer any rights or obligations in or upon any third person or entity under this Agreement. None of the parties intend to directly or substantially benefit a third party by this Agreement. The parties agree that there are no third party beneficiaries to this Agreement and that no third party shall be entitled to assert a claim against any of the parties based upon this Agreement. Nothing herein shall be construed as consent by an agency or political subdivision of the State of Florida to be sued by third parties in any matter arising out of any contract.

3.03 **Independent Contractor.** The parties to this agreement shall at all times be acting in the capacity of independent contractors and not as an officer, employee or agent of one another. Neither party or its respective agents, employees, subcontractors or assignees shall represent to others that it has the authority to bind the other party unless specifically authorized in writing to do so. No right to SBBC retirement, leave benefits or any other benefits of SBBC employees shall exist as a result of the performance of any duties or responsibilities under this Agreement. SBBC shall not be responsible for social security, withholding taxes, and contributions to unemployment compensation funds or insurance for the other party or the other party's officers, employees, agents, subcontractors or assignees.

3.04 **Equal Opportunity Provision.** The parties agree that no person shall be subjected to discrimination because of age, race, color, disability, gender identity, gender expression marital status, national origin, religion, sex or sexual orientation in the performance of the parties' respective duties, responsibilities and obligations under this Agreement.

3.05 **M/WBE Commitment.** Throughout the term of the Agreement, VENDOR shall take commercially reasonable steps and use commercially reasonable resources to identify SBBC-certified M/WBE VENDORS who may be engaged to fulfill various aspects of the Agreement, including, for instance, without limitation, M/WBE VENDORS to provide office supplies, travel, printing, janitorial supplies/services, consulting services, trade services, installation and repair services, medical supplies, where feasible. VENDOR agrees to provide monthly reports and to conduct quarterly meetings with SBBC to discuss progress in meeting the SBBC's objectives regarding M/WBE participation, including dollars spent on M/WBE VENDORS for the quarter; and to continue to assess throughout the term of the Agreement new possibilities for M/WBE VENDOR participation suggested by SBBC. If at any time during the term the parties agree that it is reasonably feasible to include a specific dollar figure for M/WBE participation, the Agreement shall be amended to include the dollar participation objective.

3.06 **Termination.** This Agreement may be canceled with or without cause by SBBC during the term hereof upon thirty (30) days written notice to the other parties of its desire to terminate this Agreement. SBBC shall have no liability for any property left on SBBC's property by any party to this Agreement after the termination of this Agreement. Any party contracting with SBBC under this Agreement agrees that any of its property placed upon SBBC's facilities pursuant to this Agreement shall be removed within ten (10) business days following the termination, conclusion or cancellation of this Agreement and that any such property remaining upon SBBC's facilities after that time shall be deemed to be abandoned, title to such property shall pass to SBBC, and SBBC may use or dispose of such property as SBBC deems fit and appropriate.

3.07 **Default.** The parties agree that, in the event that either party is in default of its obligations under this Agreement, the non-defaulting party shall provide to the defaulting party (30) days written notice to cure the default. However, in the event said default cannot be cured within said thirty (30) day period and the defaulting party is diligently attempting in good faith to cure same, the time period shall be reasonably extended to allow the defaulting party additional cure time. Upon the occurrence of a default that is not cured during the applicable cure period, this Agreement may be terminated by the non-defaulting party upon thirty (30) days' notice. This remedy is not intended to be exclusive of any other remedy, and each and every such remedy shall be cumulative and shall be in addition to every other remedy now or hereafter existing at law or in equity or by statute or otherwise. No single or partial exercise by any party of any right, power, or remedy hereunder shall preclude any other or future exercise thereof. Nothing in this section shall be construed to preclude termination for convenience pursuant to Section 3.05.

3.08 **Annual Appropriation.** The performance and obligations of SBBC under this Agreement shall be contingent upon an annual budgetary appropriation by its governing body. If SBBC does not allocate funds for the payment of services or products to be provided under this Agreement, this Agreement may be terminated by SBBC at the end of the period for which funds have been allocated. SBBC shall notify the other party at the earliest possible time before such termination. No penalty shall accrue to SBBC in the event this provision is exercised, and SBBC shall not be obligated or liable for any future payments due or any damages as a result of termination under this section.

3.09 **Excess Funds.** Any party receiving funds paid by SBBC under this Agreement agrees to promptly notify SBBC of any funds erroneously received from SBBC upon the discovery of such erroneous payment or overpayment. Any such excess funds shall be refunded to SBBC.

3.10 **Public Records**: The following provisions are required by Section 119.0701, Florida Statutes, and may not be amended. VENDOR shall keep and maintain public records required by SBBC to perform the services required under this Agreement. Upon request from SBBC's custodian of public records, VENDOR shall provide SBBC with a copy of any requested public records or to allow the requested public records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes, or as otherwise provided by law. VENDOR shall ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the Agreement's term and following completion of the Agreement if VENDOR does not transfer the public records to SBBC. Upon completion of the Agreement, VENDOR shall transfer, at no cost, to SBBC all public records in possession of VENDOR or keep and maintain public records required by SBBC to perform the services required under the Agreement. If VENDOR transfer all public records to SBBC upon completion of the Agreement, VENDOR shall destroy any duplicate public records that are exempt or confidential and

exempt from public records disclosure requirements. If VENDOR keeps and maintains public records upon completion of the Agreement, Insert Name shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to SBBC, upon request from SBBC's custodian of public records, in a format that is compatible with SBBC's information technology systems. **IF A PARTY TO THIS AGREEMENT HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO ITS DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THE AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT 754-321-1900, REQUEL.BELL@BROWARDSCHOOLS.COM, RISK MANAGEMENT DEPARTMENT, PUBLIC RECORDS DIVISION, 600 SOUTHEAST THIRD AVENUE, FORT LAUDERDALE, FLORIDA 33301.**

3.11 **Student Records.** Notwithstanding any provision to the contrary within this Agreement, any party contracting with SBBC under this Agreement shall fully comply with the requirements of Sections 1002.22 and 1002.221, Florida Statutes; FERPA, and any other state or federal law or regulation regarding the confidentiality of student information and records. Each such party agrees, for itself, its officers, employees, agents, representatives, contractors or subcontractors, to fully indemnify and hold harmless SBBC and its officers and employees for any violation of this section, including, without limitation, defending SBBC and its officers and employees against any complaint, administrative or judicial proceeding, payment of any penalty imposed upon SBBC, or payment of any and all costs, damages, judgments or losses incurred by or imposed upon SBBC arising out of a breach of this covenant by the party, or an officer, employee, agent, representative, contractor, or sub-contractor of the party to the extent that the party or an officer, employee, agent, representative, contractor, or sub-contractor of the party shall either intentionally or negligently violate the provisions of this section or of Sections 1002.22 and/or 1002.221, Florida Statutes.

3.12 **Compliance with Laws.** Each party shall comply with all applicable federal state and local laws, SBBC policies codes, rules and regulations in performing its duties, responsibilities and obligations pursuant to this Agreement.

3.13 **Place of Performance.** All obligations of SBBC under the terms of this Agreement are reasonably susceptible of being performed in Broward County, Florida and shall be payable and performable in Broward County, Florida.

3.14 **Governing Law and Venue.** This Agreement shall be interpreted and construed in accordance with and governed by the laws of the State of Florida. Any controversies or legal problems arising out of this Agreement and any action involving the enforcement or interpretation of any rights hereunder shall be submitted to the jurisdiction of the State courts of the Seventeenth Judicial Circuit of Broward County, Florida.

3.15 **Entirety of Agreement.** This document incorporates and includes all prior negotiations, correspondence, conversations, agreements and understandings applicable to the matters contained herein and the parties agree that there are no commitments, agreements or understandings concerning the subject matter of this Agreement that are not contained in this document. Accordingly, the parties agree that no deviation from the terms hereof shall be predicated upon any prior representations or agreements, whether oral or written.

3.16 **Binding Effect.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and assigns.

3.17 **Assignment.** Neither this Agreement nor any interest herein may be assigned, transferred or encumbered by any party without the prior written consent of the other party. There shall be no partial assignments of this Agreement including, without limitation, the partial assignment of any right to receive payments from SBBC.

3.18 **Incorporation by Reference. Attachments A-C,** attached hereto and referenced herein shall be deemed to be incorporated into this Agreement by reference.

3.19 **Captions.** The captions, section designations, section numbers, article numbers, titles and headings appearing in this Agreement are inserted only as a matter of convenience, have no substantive meaning, and in no way define, limit, construe or describe the scope or intent of such articles or sections of this Agreement, nor in any way affect this Agreement and shall not be construed to create a conflict with the provisions of this Agreement.

3.20 **Severability.** In the event that any one or more of the sections, paragraphs, sentences, clauses or provisions contained in this Agreement is held by a court of competent jurisdiction to be invalid, illegal, unlawful, unenforceable or void in any respect, such shall not affect the remaining portions of this Agreement and the same shall remain in full force and effect as if such invalid, illegal, unlawful, unenforceable or void sections, paragraphs, sentences, clauses or provisions had never been included herein.

3.21 **Preparation of Agreement.** The parties acknowledge that they have sought and obtained whatever competent advice and counsel as was necessary for them to form a full and complete understanding of all rights and obligations herein and that the preparation of this Agreement has been their joint effort. The language agreed to herein expresses their mutual intent and the resulting document shall not, solely as a matter of judicial construction, be construed more severely against one of the parties than the other.

3.22 **Amendments.** No modification, amendment, or alteration in the terms or conditions contained herein shall be effective unless contained in a written document prepared with the same or similar formality as this Agreement and executed by each party hereto.

3.23 **Waiver.** The parties agree that each requirement, duty and obligation set forth herein is substantial and important to the formation of this Agreement and, therefore, is a material term hereof. Any party's failure to enforce any provision of this Agreement shall not be deemed a waiver of such provision or modification of this Agreement unless the waiver is in writing and signed by the party waiving such provision. A written waiver shall only be effective as to the specific instance for which it is obtained and shall not be deemed a continuing or future waiver.

3.24 **Force Majeure.** Neither party shall be obligated to perform any duty, requirement or obligation under this Agreement if such performance is prevented by fire, hurricane, earthquake, explosion, wars, sabotage, accident, flood, acts of God, strikes, or other labor disputes, riot or civil commotions, or by reason of any other matter or condition beyond the control of either party, and which cannot be overcome by reasonable diligence and without unusual expense ("Force Majeure"). In no event shall a lack of funds on the part of either party be deemed Force Majeure.

3.25 **Survival.** All representations and warranties made herein, indemnification obligations, obligations to reimburse SBBC, obligations to maintain and allow inspection and audit of records and

property, obligations to maintain the confidentiality of records, reporting requirements, and obligations to return public funds shall survive the termination of this Agreement.

3.26 **Contract Administration.** SBBC has delegated authority to the Superintendent of Schools or his/her designee to take any actions necessary to implement and administer this Agreement.

3.27 **Liability.** This section shall survive the termination of all performance or obligations under this Agreement and shall be fully binding until such time as any proceeding brought on account of this Agreement is barred by any applicable statute of limitations.

A. By SBBC: SBBC agrees to be fully responsible up to the limits of Section 768.28, Florida Statutes, for its acts of negligence, or its employees' acts of negligence when acting within the scope of their employment and agrees to be liable for any damages resulting from said negligence.

B. By VENDOR: VENDOR agrees to indemnify, hold harmless and defend SBBC, its agents, servants and employees from any and all claims, judgments, costs, and expenses including, but not limited to, reasonable attorney's fees, reasonable investigative and discovery costs, court costs and all other sums which SBBC, its agents, servants and employees may pay or become obligated to pay on account of any, all and every claim or demand, or assertion of liability, or any claim or action founded thereon, arising or alleged to have arisen out of the products, goods or services furnished by VENDOR, its agents, servants or employees; the equipment of VENDOR, its agents, servants or employees while such equipment is on premises owned or controlled by SBBC; or the negligence of VENDOR or the negligence of VENDOR'S agents when acting within the scope of their employment, whether such claims, judgments, costs and expenses be for damages, damage to property including SBBC's property, and injury or death of any person whether employed by VENDOR, SBBC or otherwise.

3.28 **Authority.** Each person signing this Agreement on behalf of either party individually warrants that he or she has full legal power to execute this Agreement on behalf of the party for whom he or she is signing, and to bind and obligate such party with respect to all provisions contained in this Agreement.

IN WITNESS WHEREOF, the Parties hereto have made and executed this Agreement on the date first above written.

FOR SBBC

(Corporate Seal)

THE SCHOOL BOARD OF BROWARD COUNTY, FLORIDA

By _____
Nora Rupert, Chair

ATTEST:

_____
Robert W. Runcie, Superintendent of Schools

Approved as to Form and Legal Content:

Janette M. Smith Digitally signed by Janette M. Smith
Date: 2018.01.12 12:47:45 -05'00'

_____
Office of the General Counsel

FOR VENDOR

(Corporate Seal)

ATTEST:

PERFORMANCE MATTERS LLC

By _____
Adam Klaber, Chief Executive Officer

_____
, Secretary

-or-

_____
Witness

_____
Witness

The Following Notarization is Required for Every Agreement Without Regard to Whether the Party Chose to Use a Secretary's Attestation or Two (2) Witnesses.

STATE OF Utah

COUNTY OF Salt Lake

The foregoing instrument was acknowledged before me this 4th day of January, 2018 by Adam Klaber of
Name of Person
Performance Matters LLC, on behalf of the corporation/agency.
Name of Corporation or Agency
He/She is personally known to me or produced _____ as identification and did/did not first take an oath.
Type of Identification

My Commission Expires:

May 27, 2019

(SEAL)

EFFROSENE SERGAKIS
Notary Public, State of Utah
Commission # 683747
My Commission Expires
May 27, 2019

_____
Signature – Notary Public

Effrosene Sergakis
Printed Name of Notary

683747
Notary's Commission No.

ATTACHMENT A

COST OF SERVICES

YEAR 1	Unit	Count	Unit Price	Total
Software License Package: - PD Management System CHOICE (July 1, 2018 – June 30, 2019) - Due upon invoice to be paid no earlier July 1, 2018.	Per User	50,000	$7.75	$387,500
Implementation Services (Due upon execution) - Planning - Design/Build - Interface Development - Customized Reporting - Conversion - Testing - Implementation/Installation - Support	 Days Included Included Included Included Included $2,500 Included	 20 1	 $1,400 $2,500	 $28,000 $2,500
Training Costs: Due upon invoice to be paid no earlier July 1, 2018. - Face to face *How many facilitators per session?* *Maximum Attendees per session?* - Webinars - Online training *How many facilitators per session?* *How many simultaneous sessions?* - Other training delivery models PD Custom Documentation Custom Video	 Per Day *Each* *Total* Per Hour *Each* *Per Session* Each Each	 7 *1* *40* *1* *40* 1 1	 $2,400 $325 $500 $800	 $16,800 $325 $500 $800
			Year 1 -Total	**$436,425**

YEAR 2	Unit	Count	Unit Price	Total
Software License Package: - PD Management System CHOICE (July 1, 2019 – June 30, 2020)	Per User	50,000	$7.75	$387,500
- Support	Included			
			Year 2 -Total	**$387,500**

YEAR 3	Unit	Count	Unit Price	Total
Software License Package: - PD Management System CHOICE (July 1, 2020 – June 30, 2021)	Per User	50,000	$7.75	$387,500
- Support	Included			
			Year 3 -Total	**$387,500**

GRAND TOTAL $1,211,425

OPTIONAL	Unit	Count	Unit Price	Total
Development of Customizations:				
- Hourly Rate	Per Hour		$225.00	
- Custom Reports (Rate per Report)	Each		$185.00	
- **Optional** M/WBE Onsite Implementation Resources	Each		$100,000	

ATTACHMENT B

SERVICE CHANGE REQUEST FORM ("SCR")

Performance Matters LLC ("PM") a Utah limited liability company, located at: 7730 South Union Park Avenue, Suite 500 Sandy, Utah 84047		***Customer Name*** **("Customer")** located at: Address1 City, State Zip Code	
SCR Effective Date		**SCR Number**	
PM contact:		**Client contact:**	

Effective on the SCR Effective Date, this SCR is incorporated by this reference into the [***insert name of Agreement***] dated _____, 20__ ("Agreement") by and between the parties and is governed by the terms and provisions of that Agreement. Except as amended or supplemented by this SCR, the terms and conditions of the Agreement remain in full force and effect.

1. The Payment Remittance Address is Performance Matters, Accounts Receivable, 8860 East Chaparral Road, Suite 100, Scottsdale, AZ 85250. All payments should be directed to Accounts Receivable at this address. Any billing questions may be sent via email to <accounting@performancematters.com>.

Description of SCR Change to Agreement:

Accepted and Agreed as of SCR Effective Date.

[*Customer*]	**Performance Matters LLC**
Signed:	Signed:
Name:	Name:
Title:	Title:
Date:	Date:

ATTACHMENT C

INFORMATION SECURITY GUIDELINES

1 Introduction

This document provides the foundation and strategic framework for the protection of Broward County Public Schools (BCPS) information and information systems. BCPS management, users, system developers and security practitioners should use these guidelines to gain an understanding of the basic security requirements BCPS information systems should contain.
These information security guidelines are composed of generally accepted security principles as well as common security practices:

- **Security principles** address information systems security from a high-level viewpoint. These principles must be considered when developing new computer applications and when establishing or updating information security policies. Principles are expressed broadly, encompassing areas such as accountability, cost effectiveness and integration.
- **Security practices** guide the organization in establishing the specific control objectives and security procedures that comprise an effective security program. These security practices are the common ground all BCPS systems must share.

This document has two distinct uses. The chapter covering principles is to be used by all levels of BCPS management and by those individuals responsible for information security at the system level and organization level. The principles are intended as a guide when creating program policy or reviewing existing policy. The common practices are intended as a reference guide. The goal of this document is to provide a common baseline of requirements that shall be used within BCPS by managers, users and information security personnel.

2 Security Principles

The principles contained in this section provide an anchor on which BCPS should base its IT security program. These principles are intended to guide BCPS personnel when creating new systems, practices, or policies. They are based on the National Institute of Standards and Technology (NIST) Special Publication 800-series, a broadly reviewed and accepted set of security frameworks.

- **Information security supports the mission of BCPS.** Information security's role is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps BCPS protect its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.
- **Information security is an integral element of sound management.** Information systems are critical assets that support the mission of an organization. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, or employees.
- **Information security should be cost-effective.** The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value

of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm.

- **Information security responsibilities and accountability should be made explicitly.** The responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be explicit.
- **Information security requires a comprehensive and integrated approach.** Providing effective information security requires a comprehensive approach that considers a variety of areas both within and outside of IT. This comprehensive approach extends throughout the entire information life cycle. To work effectively, security controls often depend upon the proper functioning of other controls.
- **Information security should be assessed periodically.** Information systems and the environments in which they operate are dynamic, and changes in the system or the environment can create new vulnerabilities.

3 Information Security Practices

The following information security guidelines, in conjunction with appropriate state and federal statutes, will serve as a foundation and strategic framework for the protection of Broward County Public Schools (BCPS) information systems.

3.1 Information Security Policy

SBBC Policy 5306, *School and District Technology Usage*, grants the Superintendent of Schools (or designee) sole responsibility for "establishing and maintaining procedures for disabling or otherwise modifying any technology protection measures."[1] All individuals who use District-owned or leased technology, applications, networks or telecommunications infrastructure and systems agree to abide by the terms and tenets of SBBC Policy 5306.

This document, *Information Security Guidelines*, is incorporated by reference to SBBC Policy 5306, requiring all users to follow and abide by the security practices contained in this section. This includes all District staff, temporary help, volunteers, students, auditors, consultants and vendors seeking access to BCPS computer resources.

In addition to SBBC Policy 5306 and the *Information Security Guidelines* (this document), other supplemental guidance, issue-specific policies (to address compliance issues, for example) and system-specific policies may be implemented and incorporated by reference to these guidelines. Supplemental guidance and policies are referenced throughout this document and indexed in the appendix.

3.2 Risk Management

Risk management is an ongoing process of identifying, assessing and responding to the possibility of something adverse happening. BCPS employs a structured information security risk management process based on NIST Special Publication 800-39, *Managing Information Security Risk*.[2] As it relates to the protection of BCPS information and systems infrastructure, any BCPS data (regardless of where or how it is stored or managed) should be considered in-scope for purposes of risk assessment and risk mitigation.

---

[1] SBBC Policy 5306, *School and District Technology Usage*, Section 3s, http://web/sbbcpolicies/docs/P5306.000.pdf

[2] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

3.3 Life Cycle Planning

Security, like any other aspect of an information system, is best managed if planned for throughout the development life cycle. During the development of new systems for BCPS, security activities should be integrated during each of the development phases. Regardless of the methodology employed in building the system, a security plan for the development effort should be utilized to ensure that security is considered during all phases of the effort.
BCPS endeavors to leverage a structured life cycle planning process. At the same time, however, it is acknowledged that many IT projects and initiatives, such as service-oriented architectures, infrastructure projects or alternative project management methodologies (e.g. Agile) require tailored approaches to integrating security considerations.

3.4 Personnel / User Issues

A broad range of security issues relate to how BCPS personnel and non-employee users interact with BCPS information systems. Determining the appropriate level of systems access and the authorities required for individuals to do their job is critical to securing the systems environment.

3.4.1 Staffing

Early in the process of defining a new position, security issues should be identified and addressed. Once a position has been broadly defined, the responsible supervisor should determine the type of systems access needed for the position. Two general security rules should be applied when granting access:

- **Separation of duties.** Roles and responsibilities should be divided so that a single individual cannot subvert a critical process.
- **Least privilege.** Users should only be granted access to functions they need to perform their official duties.

3.4.2 User Administration

BCPS ensures effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access by requiring the following for all BCPS applications and systems:

- **User Account Management.** BCPS has a standard process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.
- **Audit and Management Reviews.** It is necessary to periodically review user account management on a system. Reviews should examine the levels of access everyone has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews should be conducted on an application-by-application basis and a system wide basis.
- **Detecting Unauthorized/Malicious Activities.** All BCPS systems should have mechanisms besides auditing and analysis of audit trails to detect unauthorized and/or malicious acts.

3.5 Contingency Planning

Contingency planning addresses how to keep the District's critical functions operating in the event of disruptions, both large and small.
All BCPS mission-critical and business-critical functions should be identified in a contingency business plan. Each of the functions catalogued in the business plan should have an appropriate priority assigned to it along with the approval of senior management.
For all the critical functions listed in the contingency business plan, personnel *who have knowledge of how each function is performed* should analyze and identify the resources needed to perform that function. Care should be taken to include areas where functions may overlap areas of responsibility, utilize common resources (such as personnel or infrastructure) and/or critical processing timeframes.
Many of the tasks related to the implementation and maintenance of contingency plans are ongoing. These tasks include making appropriate preparations, documenting recovery procedures, training of personnel and testing/revising elements of the plan periodically.

3.6 Security Incident Handling

An IT security incident can result from a computer virus, other malicious code, unauthorized access to systems or a data breach. Although some elements of security incident handling can be addressed by the BCPS contingency plan, the organization also maintains specific security incident handling guidelines,[3] as well as a Cyber Security Incident Response Team (CSIRT). The objectives of these guidelines and the CSIRT are to provide the ability to respond quickly and effectively to incidents, contain damage from incidents and prevent future damage.

3.7 Security Awareness and Training

Effective computer security awareness and training requires proper planning, implementation, maintenance, and periodic evaluation. BCPS provides appropriate training to all personnel and non-employee contractors who interact with BCPS systems and data.
All users of BCPS systems must agree and adhere to the Technology Usage Policy.[4]
BCPS evaluates elements of its security awareness and training periodically, and endeavors to ascertain how much information is retained by personnel, to what extent information security procedures are being followed, and general attitudes toward information security.

3.8 IT Support and Operations Security

IT systems administration and tasks external to IT systems (such as maintaining documentation) are critical to protecting BCPS information. Systems administration functions, maintenance accounts and other special modes of IT systems operation can inflict great harm on the confidentiality, integrity or availability of a system or systems infrastructure. To that end, BCPS places special security considerations around these elevated functions:

3.8.1 User Support

Systems support and operations staff must provide assistance to users through the help desk. Support personnel must be trained to be able to identify security problems, respond appropriately, and inform appropriate individuals.

[3] http://www.browardschools.com/SiteMedia/Docs/Policies/security-incident-handling-guidelines-011317.pdf
[4] http://web/sbbcpolicies/docs/P5306,000.pdf

3.8.2 Software support

Controls are placed on system software commensurate with the risk. The controls include:

- **Policies for loading and executing new software on a system.** Executing new software can lead to viruses, unexpected software interactions, or software that may subvert or bypass security controls.
- **Use of powerful system utilities.** System utilities can compromise the integrity of operating systems and logical access controls.
- **Authorization of system changes.** This involves the protection of software and backup copies and can be done with a combination of logical and physical access controls.
- **License management.** All BCPS software should be properly licensed, and all BCPS-owned systems including end-user systems such as desktops and mobile devices are subject to periodic audit to ensure that no illegal software is being used.

3.8.3 Configuration Management

Configuration management should ensure that changes to the system do not unintentionally or unknowingly diminish security. The goal is to know how changes will affect system security.

3.8.4 Software Updates

All BCPS systems should be updated as needed to eliminate known security vulnerabilities. The Information and Technology Department has the right to disable and restrict the use of any application or device that cannot be upgraded, updated or patched to eliminate known security vulnerabilities. Machines maintained by the Information and Technology Department to provide any kind of specialized services are not exempt from this practice.

3.8.5 Backups

It is critical to back up software and data. Frequency of backups will depend upon how often data changes and how important those changes are. Program managers should be consulted to determine what backup schedule is appropriate. Backup copies should be tested to ensure they are usable. Backups should be stored securely.

3.8.6 Documentation

All aspects of computer support and operations should be documented to ensure continuity and consistency. Security documentation should be designed to fulfill the needs of the different types of people who use it. The security of a system also needs to be documented, including security plans, contingency plans, and security policies and procedures.

3.8.7 Maintenance

Only authorized personnel should be permitted to perform maintenance on a BCPS system.

3.8.8 Standardized Log-on Banner

Prior to user authentication, BCPS systems should display a banner warning that use of the system is restricted to authorized people.

3.9 Physical and Environmental Security

Physical and environmental security controls are implemented to protect BCPS IT facilities housing system resources, the system resources themselves, and the facilities used to support their operation. These controls are designed to prevent interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

The School Board of Broward County has directed the Special Investigative Unit (SIU) to be responsible for the investigation of all incidents that occur in BCPS facilities.[5]

3.10 Identification and Authentication

Identification and Authentication refers to the technical measures that prevent unauthorized people or processes from accessing an IT system. Generally, access control principles require that the system can identify and differentiate among users. Similarly, user accountability principles require that all activities on an IT system be attributable to specific individuals. Therefore, all BCPS systems must have the ability to identify users.

3.10.1 Identification

Identification is how a user provides a claimed identity to the system. The most common form of this identification is the user ID. The following should be considered when using user IDs:

- **Unique Identification.** Users should be required to identify themselves uniquely before being allowed to perform any actions on a BCPS system.
- **Correlate Actions to Users.** BCPS systems should internally maintain the identity of all active users and be able to link actions to specific users.
- **Maintenance of User IDs.** Identification data must be kept current by adding new users and deleting former users.

3.10.2 Authentication

Authentication is the means of establishing the validity of this claim. Generally, account passwords are used for this purpose, though other means (e.g. SSL certificates, tokens, biometrics) are also commonly used. The following should be considered:

- **Require Users to Authenticate.** Users should be required to authenticate their claimed identities on BCPS systems. It may be desirable for users to authenticate themselves with a single log-in. This requires the user to authenticate themselves only once and then be able to access a wide variety of applications and data available on local and remote systems.
- **Restrict Access to Authentication Data.** Authentication data should be protected with access controls and one-way encryption to prevent unauthorized individuals, including system administrators, or hackers from obtaining the data.
- **Secure Transmission of Authentication Data.** Authentication data should be protected when transmitted over public or shared data networks.
- **Limit Log-on Attempts.** The number of log-on attempts should be limited with automatic lockouts after a set number of failed log-on attempts to prevent guessing of authentication data.

[5] http://www.broward.k12.fl.us/sbbcpolicies/docs/P2302.000.pdf

- **Secure Authentication Data as it is Entered.** Authentication data should be protected as it is entered into any BCPS system, including suppressing the display of the password as it is entered.
- **Administer Data Properly.** Authentication data and tokens should be carefully administered including procedures to disable lost or stolen passwords or tokens and monitoring systems to look for stolen or shared accounts.

3.10.3 Passwords

All BCPS systems utilizing passwords for authentication should follow the established password policy guidance.

3.11 Logical Access Control

Logical access controls are the system-based means by which the ability to do something with BCPS data (such as use, change or view) is explicitly enabled or restricted in some way. Logical access controls can prescribe not only who or what (e.g., in the case of a system process) is to have access to a specific system resource but also the type of access that is permitted.
BCPS implements logical access control based on policy made by the management official responsible for a system, application, subsystem, or group of systems.

3.11.1 Access Criteria

Security administrators should control access to resources based on the following access criteria, as appropriate:

- **Identity (user ID).** The identity should be unique to support individual accountability.
- **Roles.** Access to information should also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access.
- **Location.** Access to system resources may be based on physical or logical location.
- **Time.** Time-of-day and day-of-week/month restrictions are another type of limitation on access.
- **Transaction.** Access to BCPS data could be granted only for the duration of a transaction, such as an account inquiry requiring an account number and PIN.
- **Service Constraints.** Service constraints refer to those restrictions that depend upon licensing or other similar limitations, such as the maximum number of concurrent users.
- **Access Modes.** Common access modes, which can be used in both operating or application systems, include read, write, execute, and delete. Other specialized access modes (more often found in applications) include create or search.

3.11.2 Access Control Mechanisms

In addition to criteria-based access controls, BCPS maintains both internal and external access control mechanisms to restrict access to system, network and infrastructure resources:

- **Access control lists (ACLs).** ACLs are a register of users (including groups, machines and system processes) who have been given permission to use a system resource and the types of access they have been permitted.

- **Constrained User Interfaces.** Access to specific functions are restricted by never allowing users to request information, functions, or other resources for which they do not have access.
- **Encryption.** Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key.
- **Secure Gateways/Firewalls.** Secure gateways block or filter access between two networks, often between a private network and a larger, more public network such as the Internet. Secure gateways allow internal users to connect to external networks while protecting internal systems from compromise.

3.12 Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

System audit trails should include sufficient information to establish what events occurred and who (or what) caused them. Audit trails should be protected from unauthorized access or tampering. Access to online audit logs should be strictly controlled, and the confidentiality of audit trail information should be protected. Audit trails should be reviewed periodically.