

**AGREEMENT****GOODS AND SERVICES AGREEMENT**

**THIS GOODS AND SERVICES AGREEMENT** is made as of the 11<sup>th</sup> day of October, 2022 (effective date). By and between Pinellas County, a political subdivision of the State of Florida ("County"), and Revere Control Systems Inc, located in Birmingham, Alabama ("Contractor"), (individually, "Party," collectively, "Parties").

**WITNESSETH:**

**WHEREAS**, the County requested proposals pursuant to Contract No. 22-0427-B-BW ("ITB") for Instrumentation Control & Monitoring Systems Repair, Maintenance and Training & Consulting Support; and

**WHEREAS**, based upon the County's assessment of Contractor's proposal, the County selected the Contractor to provide the Services as defined herein; and

**WHEREAS**, Contractor represents that it has the experience and expertise to provide Goods and perform the Services as set forth in this Agreement.

**NOW, THEREFORE**, in consideration of the above recitals, the mutual covenants, agreements, terms and conditions herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby mutually acknowledged, the Parties agree as follows:

**1. Definitions**

- A. **"Agreement"** means this Agreement, including all Exhibits, which are expressly incorporated herein by reference, and any amendments thereto.
- B. **"County Confidential Information"** means any County information deemed confidential and/or exempt from Section 119.07, Florida Statutes, and Section 24(a), Article 1 of the Florida Constitution, or other applicable law, including, but not limited to data or information referenced in this Goods and Services Agreement, and any other information designated in writing by the County as County Confidential Information.
- C. **"Contractor Confidential Information"** means any Contractor information that is designated as confidential and/or exempt by Florida's public records law, including information that constitutes a trade secret pursuant to Chapter 688, Florida Statutes, and is designated in this Agreement or in writing as a trade secret by Contractor (unless otherwise determined to be a public record by applicable Florida law). Notwithstanding the foregoing, Contractor Confidential Information does not include information that: (i) becomes public other than as a result of a disclosure by the County in breach of the Agreement; (ii) becomes available to the County on a non-confidential basis from a source other than Contractor, which is not prohibited from disclosing such information by obligation to Contractor; (iii) is known by the County prior to its receipt from Contractor without any obligation or confidentiality with respect thereto; or (iv) is developed by the County independently of any disclosures made by Contractor.
- D. **"Contractor Personnel"** means all employees of Contractor, and all employees of subcontractors of Contractor, including, but not limited to temporary and/or leased employees, who are providing the Services at any time during the project term.
- E. **"Services"** means the work, duties and obligations to be carried out and performed safely by Contractor under this Agreement, as described throughout this Agreement and as specifically described in the Statement of Work Exhibit attached hereto and incorporated herein by reference. As used in this Agreement, Services shall include any component task, subtask, service, or function inherent, necessary, or a customary part of the Services, but not specifically described in this Agreement, and shall include the provision of all standard day-to-day administrative, overhead, and internal expenses, including costs of bonds and insurance as required herein, labor, materials, equipment, safety equipment, products, office supplies, consumables, tools, postage, computer hardware/software, telephone charges, copier usage, fax charges, travel, lodging, and per diem and all other costs required to perform Services except as otherwise specifically provided in this Agreement.

**2. Execution of Agreement**

The execution of this Agreement is expressly limited by the Terms and Conditions hereon. County and the Contractor are not bound by additional provisions or provisions at variance herewith that may appear in the Contractor's quotation, estimate, scope of work, or any other such related documents, acknowledgement in force, or any other communication from Contractor to or from County unless such provision is expressly set forth herein.

**AGREEMENT****3. Conditions Precedent**

This Agreement, and the Parties' rights and obligations herein, are contingent upon and subject to the Contractor securing and/or providing the performance security, if required, and the insurance coverage(s) required, within 10 days of the Effective Date. No Services shall be performed by the Contractor and the County shall not incur any obligations of any type until Contractor satisfies these conditions. Unless waived in writing by the County, in the event the Contractor fails to satisfy the conditions precedent within the time required herein, the Agreement shall be deemed not to have been entered into and shall be null and void.

**4. Services**

- A. **Services** - The County retains Contractor, and Contractor agrees to provide the Services. All Services shall be performed to the satisfaction of the County and shall be subject to the provisions and terms contained herein and the Exhibits attached hereto.
- B. **Services Requiring Prior Approval** - Contractor shall not commence work on any Services requiring prior written authorization in the Statement of Work without approval from the Utilities SCADA and Security Systems Manager.
- C. **Additional Services** - From the Effective Date and for the duration of the project, the County may elect to have Contractor perform Services that are not specifically described in the Statement of Work attached hereto but are related to the Services ("Additional Services"), in which event Contractor shall perform such Additional Services for the compensation specified in the Statement of Work attached hereto. Contractor shall commence performing the applicable Additional Services promptly upon receipt of written approval as provided herein.
- D. **De-scoping of Services** - The County reserves the right, in its sole discretion, to de-scope Services upon written notification to the Contractor by the County. Upon issuance and receipt of the notification, the Contractor and the County shall enter into a written amendment reducing the appropriate Services Fee for the impacted Services by a sum equal to the amount associated with the de-scoped Services as defined in the payment schedule in this Agreement, if applicable, or as determined by mutual written consent of both Parties based upon the scope of work performed prior to issuance of notification.
- E. **Independent Contractor Status and Compliance with the Immigration Reform and Control Act** - Contractor is and shall remain an independent contractor and is neither agent, employee, partner, nor joint venturer of County. Contractor acknowledges that it is responsible for complying with the provisions of the Immigration Reform and Control Act of 1986 located at 8 U.S.C. 1324, et seq, and regulations relating thereto, as either may be amended from time to time. Failure to comply with the above provisions shall be considered a material breach of the Agreement.
- F. **Non-Exclusive Services** - Award of this Agreement imposes no obligation on the County to utilize the Contractor for all goods and/or services of this type, which may develop during the agreement period. This is a non-exclusive Agreement. During the term of this Agreement, and any extensions thereof, the County reserves the right to contract for another provider for similar goods and/or services as it determines necessary in its sole discretion.
- G. **Project Monitoring** - During the term of the Agreement, Contractor shall cooperate with the County, either directly or through its representatives, in monitoring Contractor's progress and performance of this Agreement.

**5. Term of Agreement**

- A. **Initial Term** - The term of this Agreement shall commence on:

☒ **September 23, 2022**, and shall remain in full force and for sixty (60) months, or until termination of the Agreement, whichever occurs first.

- B. **Term Extension**

☒ The Parties may extend the term of this Agreement for two (2) additional twelve (12) month period(s) pursuant to the same terms, conditions, and pricing set forth in the Agreement by mutually executing an amendment to this Agreement, as provided herein.

**6. Orders**

Within the term of this Agreement, County may place one or more orders for goods and/or services at the prices listed on the Price Schedule Exhibit attached hereto, and which is incorporated by reference hereto.



AGREEMENT
-----------

**7. Delivery / Claims**

Prices on the Schedule of Prices are F.O.B. Destination, FREIGHT INCLUDED and unloaded to location(s) within Pinellas County. Actual delivery address(es) will be identified at time of order. Contractor will be responsible for making any and all claims against carriers for missing or damaged items.

**8. Inspection**

In County's sole discretion, goods rejected due to inferior quality or workmanship will be returned to Contractor at Contractor's expense and are not to be replaced except upon receipt of written instructions from County.

**9. Material Quality**

All goods and materials purchased and delivered pursuant to this Agreement will be of first quality and not damaged and/or factory seconds. Any materials damaged or not in first quality condition upon receipt must be exchanged within 24 hours of notice to the Contractor at no charge to County.

**10. Material Safety Data**

In accordance with OSHA Hazardous Communications Standards, it is the Contractor seller's duty to advise if a product is a toxic substance and to provide a Material Safety Data Sheet at time of delivery.

**11. Purchase Order Number**

Each order will contain the Purchase Order Number applicable to this Agreement, and such Purchase Order Number must appear on all packing slips, invoices and all correspondence relating to the Order. County will not be responsible for goods delivered without a Purchase Order Number.

**12. Variation in Quantity**

County assumes no liability for goods or materials produced, processed or shipped in excess of the amounts ordered pursuant to the terms of this Agreement.

**13. Warranty**

Seller warrants that the goods are of first quality and as described in Prices Schedule. All manufacturer, producer or seller warranties offered to any other purchaser are expressly available and applicable to County.

**14. Compensation and Method of Payment**

- A. **Goods and Services Fee** - As total compensation for the Goods and Services, the County shall pay the Contractor the sums as provided in this Section Compensation and Method Payment ("Goods and Services Fee"), pursuant to the terms and conditions as provided in this Agreement. It is acknowledged and agreed by Contractor that this compensation constitutes a limitation upon County's obligation to compensate Contractor for such Goods and Services required by this Agreement but does not constitute a limitation upon Contractor's obligation to provide Goods and perform all of the Services required by this Agreement. In no event will the Goods and Services Fee paid exceed the not-to-exceed sums set out in subsections below, unless the Parties agree to increase this sum by written amendment as authorized in the Amendment Section of this Agreement.
- B. **Spending Cap and Payment Structure** - The County agrees to pay the Contractor the total not-to-exceed sum of \$836,410.00, with an annual expenditure which will not exceed \$350,000.00 in any given fiscal year for the duration of the Agreement, and not-to-exceed the full contract expenditure for the sixty (60) month term period, for Goods and Services completed and accepted herein, payable on a fixed-fee basis for the deliverables as set out in Exhibit C, upon submittal of an invoice as required herein. Unit prices listed in Exhibit C shall be held firm for the initial contract term.
- C. **Term Extension Price Adjustment** - Term extensions will allow for price adjustments (Decrease/Increase) in an amount not to exceed the average of the Consumer Price Index (CPI) or **2.0%**, whichever is less, for all Urban Consumers, Series Id: CUUR0000SA0, Not Seasonally Adjusted, Area: U.S. city average, Item: All items, Base Period: 1982-84=100 for the twelve months prior to extension. The extension shall be exercised only if all terms and conditions remain the same and the County Administrator or Director of Purchasing grants approval.

It is the vendor's responsibility to request any pricing adjustment under this provision. For any adjustment to commence on the first day of any exercised extension period, the vendor's request for adjustment should be submitted at time of the extension request from the County, utilizing the available index at the time of request. The

## AGREEMENT

vendor adjustment request should not be in excess of the relevant pricing index change. If no adjustment request is received from the vendor, the County will assume the vendor has agreed that the extension term may be exercised without pricing adjustment. Any adjustment request received after the commencement of a new extension period may not be considered.

**D. Travel Expenses**

☒ The Services Fee includes all travel, lodging and per diem expenses incurred by Contractor in performing the Services.

**E. Taxes** - Contractor acknowledges that the County is not subject to any state or federal sales, use, transportation and certain excise taxes.

**C. Payments and Invoicing** - Contractor shall submit invoices for payments due as provided herein and authorized reimbursable expenses incurred with such documentation as required by County. Invoices shall be submitted to:

☒ the designated person as set out in the Notices Section herein.

For time and materials Services, all Contractor Personnel shall maintain logs of time worked, and each invoice shall state the date and number of hours worked for Services authorized to be billed on a time and materials basis.

All payments shall be made in accordance with the requirements of Section 218.70 et seq., Florida Statutes, "The Local Government Prompt Payment Act." The County may dispute any payments invoiced by Contractor in accordance with the County's Invoice Payments Dispute Resolution Process established in accordance with Section 218.76, Florida Statutes, and any such disputes shall be resolved in accordance with the County's Dispute Resolution Process.

**15. Acceptance of Services**

For all Services deliverables that require County acceptance as provided in the Statement of Work, the County, through the Utilities SCADA and Security Systems Manager or designee, will have 10 calendar days to review the deliverable(s) after receipt or completion of same by Contractor, and either accept or reject the deliverable(s) by written notice to Revere Control Systems Inc. If a deliverable is rejected, the written notice from the County will specify any required changes, deficiencies, and/or additions necessary. Contractor shall then have 7 calendar days to revise the deliverable(s) to resubmit and/or complete the deliverable(s) for review and approval by the County, who will then have 7 calendar days to review and approve, or reject the deliverable(s); provided however, that Contractor shall not be responsible for any delays in the overall project schedule that result from the County's failure to timely approve or reject deliverable(s) as provided herein. Upon final acceptance of the deliverable(s), the County will accept the deliverable(s) in writing.

**16. Discounts**

Delay in receiving an invoice, invoicing for materials shipped ahead of specified schedule, or invoices rendered with errors or omissions will be considered just cause for County to withhold payment without losing discount privileges. Discount privilege will apply from date of scheduled delivery, the date of receipt of goods, or the date of approved invoice, whichever is later.

**17. Subcontracting/Assignment.**

**A. Subcontracting** - Contractor is fully responsible for completion of the Services required by this Agreement and for completion of all subcontractor work, if authorized as provided herein. Contractor shall not subcontract any work under this Agreement to any subcontractor other than the subcontractors specified in the proposal and previously approved by the County, without the prior written consent of the County, which shall be determined by the County in its sole discretion.

**B. Assignment**

☒ This Agreement, and all rights or obligations hereunder, shall not be assigned, transferred, or delegated in whole or in part, including by acquisition of assets, merger, consolidation, dissolution, operation of law, change in effective control of the Contractor, or any other assignment, transfer, or delegation of rights or obligations, without the prior written consent of the County. The Contractor shall provide written notice to the County within fifteen (15) calendar days of any action or occurrence assigning the Agreement or any rights or obligations hereunder as

**AGREEMENT**

described in this section. In the event the County does not consent to the assignment, as determined in its sole discretion, the purported assignment in violation of this section shall be null and void, and the County may elect to terminate this Agreement by providing written notice of its election to terminate pursuant to this provision upon fifteen (15) days notice to Contractor.

**18. Personnel**

- A. E-Verify** - The contractor and subcontractor must register with and use the E-verify system in accordance with Florida Statute 448.095. A contractor and subcontractor may not enter into a contract with the County unless each party registers with and uses the E-verify system.

If a contractor enters a contract with a subcontractor, the subcontractor must provide the contractor with an affidavit stating that the Subcontractor does not employ, contract with, or subcontract with unauthorized aliens. The contractor must maintain a copy of the affidavit for the duration of the contract.

If the County, Contractor, or Subcontractor has a good faith belief that a person or entity with which it is contracting has knowingly violated Florida Statute 448.09(1) shall immediately terminate the contract with the person or entity.

If the County has a good faith belief that a Subcontractor knowingly violated this provision, but the Contractor otherwise complied with this provision, the County will notify the Contractor and order that the Contractor immediately terminate the contract with the Subcontractor.

A contract terminated under the provisions of this section is not a breach of contract and may not be considered such. Any contract termination under the provisions of this section may be challenged to Section 448.095(2)(d), Florida Statute. Contractor acknowledges upon termination of this agreement by the County for violation of this section by Contractor, Contractor may not be awarded a public contract for at least one (1) year. Contractor acknowledges that Contractor is liable for any additional costs incurred by the County as a result of termination of any contract for a violation of this section.

Contractor or Subcontractor shall insert in any subcontracts the clauses set forth in this section, requiring the subcontracts to include these clauses in any lower tier subcontracts. Contractor shall be responsible for compliance by any Subcontractor or Lower Tier Subcontractor with the clause set forth in this section.

- B. Qualified Personnel** - Contractor agrees that each person performing Services in connection with this Agreement shall have the qualifications and shall fulfill the requirements set forth in this Agreement
- C. Approval and Replacement of Personnel** - The County shall have the right to approve all Contractor Personnel assigned to provide the Services, which approval shall not be unreasonably withheld. Prior to commencing the Services, the Contractor shall provide at least ten (10) days written notice of the names and qualifications of the Contractor Personnel assigned to perform Services pursuant to the Agreement. Thereafter, during the term of this Agreement, the Contractor shall promptly and as required by the County provide written notice of the names and qualifications of any additional Contractor Personnel assigned to perform Services. The County, on a reasonable basis, shall have the right to require the removal and replacement of any of the Contractor Personnel performing Services, at any time during the term of the Agreement. The County will notify Contractor in writing in the event the County requires such action. Contractor shall accomplish any such removal within forty-eight (48) hours after receipt of notice from the County and shall promptly replace such person with another person, acceptable to the County, with sufficient knowledge and expertise to perform the Services assigned to such individual in accordance with this Agreement. In situations where individual Contractor Personnel are prohibited by applicable law from providing Services, removal and replacement of such Contractor Personnel shall be immediate and not subject to such forty-eight (48) hour replacement timeframe and the provisions of the Termination Section of this Agreement shall apply if minimum required staffing is not maintained.

**19. Name Changes**

The Contractor is responsible for immediately notifying the County of any company name change, which would cause invoicing to change from the name used at the time of the original Agreement.

<b>AGREEMENT</b>
------------------

**20. Compliance with Laws**

Contractor shall comply with all applicable federal, state, county and local laws, ordinances, rules and regulations in the performance of its obligations under this Agreement, including the procurement of permits and certificates where required, and including but not limited to laws related to Workers Compensation, Americans with Disabilities Act (ADA), Section 504 of the Rehabilitation Act of 1973, Minority Business Enterprise (MBE), occupational safety and health and the environment, equal employment opportunity, privacy of medical records and information, as applicable. Failure to comply with any of the above provisions shall be considered a material breach of the Agreement.

**21. Applicable Law and Venue**

This Agreement and any and all purchases made hereunder shall be governed by and construed in accordance with the laws of the State of Florida (without regard to principles of conflicts of laws). The Parties agree that all actions or proceedings arising in connection with this Agreement shall be tried and litigated exclusively in the state or federal (if permitted by law and a Party elects to file an action in federal court) courts located in or for Pinellas County, Florida. This choice of venue is intended by the Parties to be mandatory and not permissive in nature, and to preclude the possibility of litigation between the Parties with respect to, or arising out of, this Agreement in any jurisdiction other than that specified in this section. Each Party waives any right it may have to assert the doctrine of forum non-conveniens or similar doctrine or to object to venue with respect to any proceeding brought in accordance with this section.

**22. Public Entities Crimes**

Contractor is directed to the Florida Public Entities Crime Act, Section 287.133, Florida Statutes, as well as Florida Statute 287.135 regarding Scrutinized Companies, and represents to County that Contractor is qualified to transact business with public entities in Florida, and to enter into and fully perform this Agreement subject to the provisions stated therein. Failure to comply with any of the above provisions shall be considered a material breach of the Agreement.

**23. Waiver**

No waiver by either Party of any breach or violation of any covenant, term, condition, or provision of this Agreement or of the provisions of any ordinance or law, shall be construed to waive any other term, covenant, condition, provisions, ordinance or law, or of any subsequent breach or violation of the same.

**24. Due Authority**

Each Party to this Agreement represents and warrants that: (i) it has the full right and authority and has obtained all necessary approvals to enter into this Agreement; (ii) each person executing this Agreement on behalf of the Party is authorized to do so; (iii) this Agreement constitutes a valid and legally binding obligation of the Party, enforceable in accordance with its terms.

**25. Termination****A. Contractor Default Provisions and Remedies of County****1. Events of Default** - Any of the following shall constitute a "Contractor Event of Default" hereunder:

- i. Contractor fails to maintain the staffing necessary to perform the Services as required in the Agreement, fails to perform the Services as specified in the Agreement, or fails to complete the Services within the completion dates as specified in the Agreement;
- ii. Contractor breaches Confidential Information Section of this Agreement;
- iii. Contractor fails to gain acceptance of goods and/or services deliverable, for 2 consecutive iterations; or
- iv. Contractor fails to perform or observe any of the other material provisions of this Agreement.

**2. Cure Provisions** - Upon the occurrence of a Contractor Event of Default as set out above, the County shall provide written notice of such Contractor Event of Default to Contractor ("Notice to Cure"), and Contractor shall have 30 calendar days after the date of a Notice to Cure to correct, cure, and/or remedy the Contractor Event of Default described in the written notice.



## AGREEMENT

3. **Termination for Cause by the County** - In the event that Contractor fails to cure a Contractor Event of Default as authorized herein, or upon the occurrence of a Contractor Event of Default as specified in Termination – Contractor Default Provisions and Remedies of County – Events of Default Section of this Agreement, the County may terminate this Agreement in whole or in part, effective upon receipt by Contractor of written notice of termination pursuant to this provision, and may pursue such remedies at law or in equity as may be available to the County.

**B. County Default Provisions and Remedies of Contractor**

1. **Events of Default** - Any of the following shall constitute a "County Event of Default" hereunder:
  - i. the County fails to make timely undisputed payments as described in this Agreement;
  - ii. the County breaches Confidential Information Section of this Agreement; or the County fails to perform any of the other material provisions of this Agreement.
2. **Cure Provisions** - Upon the occurrence of a County Event of Default as set out above, Contractor shall provide written notice of such County Event of Default to the County ("Notice to Cure"), and the County shall have thirty (30) calendar days after the date of a Notice to Cure to correct, cure, and/or remedy the County Event of Default described in the written notice.
3. **Termination for Cause by the Contractor** - In the event the County fails to cure a County Event of Default as authorized herein, Contractor may terminate this Agreement in whole or in part effective on receipt by the County of written notice of termination pursuant to this provision, and may pursue such remedies at law or in equity as may be available to the Contractor.

**C. Termination for Convenience**

1. Notwithstanding any other provision herein, the County may terminate this Agreement, without cause, by giving 30 days advance written notice to the Contractor of its election to terminate this Agreement pursuant to this provision.

**26. Time is of the Essence**

Time is of the essence with respect to all provisions of this Agreement that specify a time for performance, including the Services as described in the Exhibits attached hereto; provided, however, that the foregoing shall not be construed to limit a Party's cure period allowed in the Agreement.

**27. Confidential Information and Public Records**

- A. **County Confidential Information** - Contractor shall not disclose to any third party County Confidential Information that Contractor, through its Contractor Personnel, has access to or has received from the County pursuant to its performance of Services pursuant to the Agreement, unless approved in writing by the County Contract Manager. All such County Confidential Information will be held in trust and confidence from the date of disclosure by the County, and discussions involving such County Confidential Information shall be limited to Contractor Personnel as is necessary to complete the Services.
- B. **Contractor Confidential Information** - All Contractor Confidential Information received by the County from Contractor will be held in trust and confidence from the date of disclosure by Contractor and discussions involving such Contractor Confidential Information shall be limited to the members of the County's staff and the County's subcontractors who require such information in the performance of this Agreement. The County acknowledges and agrees to respect the copyrights, registrations, trade secrets and other proprietary rights of Contractor in the Contractor Confidential Information during and after the term of the Agreement and shall at all times maintain the confidentiality of the Contractor Confidential Information provided to the County, subject to federal law and the laws of the State of Florida related to public records disclosure. Contractor shall be solely responsible for taking any and all action it deems necessary to protect its Contractor Confidential Information except as provided herein. Contractor acknowledges that the County is subject to public records legislation, including but not limited to Chapter 119, Florida Statutes, and the Florida Rules of Judicial Administration, and that any of the County's obligations under this Section may be superseded by its obligations under any requirements of said laws.
- C. **Public Records** - Contractor acknowledges that information and data it manages as part of the services may be public records in accordance with Chapter 119, Florida Statutes and Pinellas County public records policies. Contractor agrees that prior to providing services it will implement policies and procedures to maintain, produce, secure, and retain public records in accordance with applicable laws, regulations, and County policies, including but not limited to the Section 119.0701, Florida Statutes. Notwithstanding any other provision of this Agreement relating to compensation, the Contractor agrees to charge the County, and/or any third parties requesting public

**AGREEMENT**

records only such fees allowed by Section 119.07, Florida Statutes, and County policy for locating and producing public records during the term of this Agreement.

**IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE PINELLAS COUNTY BOARD OF COUNTY COMMISSIONERS, PURCHASING AND RISK MANAGEMENT DEPARTMENT, OPERATIONS MANAGER CUSTODIAN OF PUBLIC RECORDS AT 727-464-3311, [PURCHASE@PINELLASCOUNTY.ORG](mailto:PURCHASE@PINELLASCOUNTY.ORG), PINELLAS COUNTY GOVERNMENT, PURCHASING AND RISK MANAGEMENT DEPARTMENT, OPERATIONS MANAGER, 400 S. FT. HARRISON AVE, 6TH FLOOR, CLEARWATER, FL 33756.**

**28. Audit**

Contractor shall retain all records relating to this Agreement for a period of at least 5 years after final payment is made. All records shall be kept in such a way as will permit their inspection pursuant to Chapter 119, Florida Statutes. In addition, County reserves the right to examine and/or audit such records.

**29. Digital Accessibility**

Contractor acknowledges and warrants that all digital content and services provided under this contract conforms and shall continue to conform during the Term of this Agreement to the W3C Web Content Accessibility Guidelines, version 2.0 ("WCAG 2.0") at conformance Level A and AA. If all digital content and services does not fully conform to WCAG 2.0 A and AA, Contractor shall advise Pinellas County in writing of the nonconformance prior to execution of this Agreement and shall provide Pinellas County a plan to achieve conformance to WCAG 2.0 A and AA, including but not limited to, an intended timeline for conformance. Failure to achieve conformance, as determined in Pinellas County's sole discretion, on its intended timeline shall be considered a material breach of this Agreement and grounds for termination by Pinellas County.

If during the Term of this Agreement, Contractor fails to maintain compliance with WCAG 2.0 A and AA or Pinellas County otherwise identifies an issue related to accessibility of the product (the "Accessibility Issue") that renders the product inaccessible, then Pinellas County shall notify Contractor of non-compliance. Within 30 days of Contractor's receipt of a non-compliance notice ("Notice"), Contractor and Pinellas County shall meet and mutually agree upon an appropriate timeline for resolution of the Accessibility Issue(s) ("Initial Meeting").

Should Contractor:

- i. fail to acknowledge receipt of the notice within 30 days of receipt of the Notice;
- ii. unreasonably and solely withhold agreement regarding a timeline for resolution for more than 30 days following the Initial Meeting; or
- iii. fail to materially resolve the Accessibility Issue(s) within the agreed-upon timeline,

Failure to comply with the requirements of this section shall constitute a material breach of this Agreement and shall be grounds for termination of this Agreement by Pinellas County and subject Contractor to the Liability and Insurance – Indemnification Section of this Agreement, "Indemnification."

**30. Liability and Insurance**

- A. **Insurance** - Contractor shall comply with the insurance requirements set out in the Insurance Exhibit, attached hereto and incorporated herein by reference.
- B. **Indemnification** - Contractor agrees to indemnify, pay the cost of defense, including attorney's fees, and hold harmless the County, its officers, employees and agents from all damages, suits, actions or claims, including

**AGREEMENT**

reasonable attorney's fees incurred by the County, of any character brought on account of any injuries or damages received or sustained by any person, persons, or property, or in any way relating to or arising from the Agreement; or on account of any act or omission, neglect or misconduct of Contractor; or by, or on account of, any claim or amounts recovered under the Workers' Compensation Law; or of any other laws, regulations, ordinance, order or decree; or arising from or by reason of any actual or claimed trademark, patent or copyright infringement or litigation based thereon; or for any violation of requirements of the Americans with Disabilities Act of 1990, as may be amended, and all rules and regulations issued pursuant thereto (collectively the "ADA") except when such injury, damage, or violation was caused by the sole negligence of the County.

- C. **Liability** - Neither the County nor Contractor shall make any express or implied agreements, guaranties or representations, or incur any debt, in the name of or on behalf of the other Party. Neither the County nor Contractor shall be obligated by or have any liability under any agreements or representations made by the other that are not expressly authorized hereunder. The County shall have no liability or obligation for any damages to any person or property directly or indirectly arising out of the operation by Contractor of its business, whether caused by Contractor's negligence or willful action or failure to act.
- D. **Contractor's Taxes** - The County will have no liability for any sales, service, value added, use, excise, gross receipts, property, workers' compensation, unemployment compensation, withholding or other taxes, whether levied upon Contractor or Contractor's assets, or upon the County in connection with Services performed or business conducted by Contractor. Payment of all such taxes and liabilities shall be the responsibility of Contractor.

**31. County's Funding**

The Agreement is not a general obligation of the County. It is understood that neither this Agreement nor any representation by any County employee or officer creates any obligation to appropriate or make monies available for the purpose of the Agreement beyond the fiscal year in which this Agreement is executed. No liability shall be incurred by the County, or any department, beyond the monies budgeted and available for this purpose. If funds are not appropriated by the County for any or all of this Agreement, the County shall not be obligated to pay any sums provided pursuant to this Agreement beyond the portion for which funds are appropriated. The County agrees to promptly notify Contractor in writing of such failure of appropriation, and upon receipt of such notice, this Agreement, and all rights and obligations contained herein, shall terminate without liability or penalty to the County.

**32. Survival**

The provisions of this Agreement shall survive the expiration or termination of this Agreement.

**33. Notices**

All notices, authorizations, and requests in connection with this Agreement shall be deemed given on the day they are: (1) deposited in the U.S. mail, postage prepaid, certified or registered, return receipt requested; or (2) sent by air express courier (e.g., Federal Express, Airborne, etc.), charges prepaid, return receipt requested; or (3) sent via email and addressed as set forth below, which designated person(s) may be amended by either Party by giving written notice to the other Party:

For County:

Attn: Ed Atchison

SCADA and Security Systems Manager

Pinellas County Utilities

7401 54th Avenue North

Saint Petersburg, FL 33709

[eatchison@pinellascounty.org](mailto:eatchison@pinellascounty.org)

AGREEMENT
-----------

with a copy to:

Attn: Merry Celeste

Purchasing and Risk Management Division Director

Pinellas County Purchasing Department

400 South Fort Harrison Avenue

Clearwater, FL 33756

[mceleste@pinellascounty.org](mailto:mceleste@pinellascounty.org)

Attn: Jean Mead

Business Development /Program Manager

Revere Control Systems Inc

2240 Rocky Ridge Road

Birmingham, AL 35216

[jmead@reverecontrol.com](mailto:jmead@reverecontrol.com)

**34. Conflict of Interest**

- A. The Contractor represents that it presently has no interest and shall acquire no interest, either direct or indirect, which would conflict in any manner with the performance of the Services required hereunder, and that no person having any such interest shall be employed by Contractor during the agreement term and any extensions.
- B. The Contractor shall promptly notify the County in writing of any business association, interest, or other circumstance which constitutes a conflict of interest as provided herein. If the Contractor is in doubt as to whether a prospective business association, interest, or other circumstance constitutes a conflict of interest, the Contractor may identify the prospective business association, interest or circumstance, the nature of work that the Contractor may undertake and request an opinion as to whether the business association, interest or circumstance constitutes a conflict of interest if entered into by the Contractor. The County agrees to notify the Contractor of its opinion within (10) calendar days of receipt of notification by the Contractor, which shall be binding on the Contractor.

**35. Right to Ownership**

All work created, originated and/or prepared by Contractor in performing Services pursuant to the Agreement, to the extent that such work, products, documentation, materials or information are described in or required by the Services (collectively, the "Work Product") shall be County's property when completed and accepted, if acceptance is required in this Agreement, and the County has made payment of the sums due therefore. The ideas, concepts, know-how or techniques developed during the course of this Agreement by the Contractor or jointly by Contractor and the County may be used by the County without obligation of notice or accounting to the Contractor. Any data, information or other materials furnished by the County for use by Contractor under this Agreement shall remain the sole property of the County.

**36. Amendment**

This Agreement may be amended by mutual written agreement of the Parties hereto.



<b>AGREEMENT</b>
------------------

**37. Severability**

The terms and conditions of this Agreement shall be deemed to be severable. Consequently, if any clause, term, or condition hereof shall be held to be illegal or void, such determination shall not affect the validity or legality of the remaining terms and conditions, and notwithstanding any such determination, this Agreement shall continue in full force and effect unless the particular clause, term, or condition held to be illegal or void renders the balance of the Agreement impossible to perform.

**38. No Third-Party Beneficiary**

The Parties hereto acknowledge and agree that there are no third party beneficiaries to this Agreement. Persons or entities not a party to this Agreement may not claim any benefit from this Agreement or as third party beneficiaries hereto.

**39. Force Majeure**

"Force Majeure Event" means any act or event that (i) prevents a Party (the "Nonperforming Party") from performing its obligations or satisfying a condition to the other Party's (the "Performing Party") obligations under this Agreement, (ii) is beyond the reasonable control of and not the fault of the Nonperforming Party, and (iii) the Nonperforming Party has not, through commercially reasonable efforts, been able to avoid or overcome. Force Majeure Event(s) do not include economic hardship, changes in market conditions or insufficiency of funds. If a Force Majeure Event occurs, the Nonperforming Party is excused from the performance and thereby prevented from satisfying any conditions precedent to the Performing Party's performance that cannot be satisfied, in each case to the extent limited or prevented by the Force Majeure Event. The Nonperforming Party must promptly notify the Performing Party upon the occurrence of a Force Majeure Event. When the Nonperforming Party is able to resume its performance or satisfy the conditions precedent to the Performing Party's obligations, the Nonperforming Party will resume performance under this Agreement without undue delay. Each Party will use commercially reasonable efforts to mitigate the effect of a Force Majeure Event.

**40. Order of Precedence**

All Exhibits attached and listed below are incorporated in their entirety into, and form part of this Agreement and will have priority in the order listed

- A. Pinellas County Goods and Services Agreement
- B. Exhibit A - Statement of Work
- C. Exhibit B - Insurance Requirements
- D. Exhibit C - Payment Schedule
- E. Exhibit D - Payment/Invoices
- F. Exhibit E - Dispute Resolution for Pinellas County Board of County Commissioners In Matters of Invoice Payments
- G. Exhibit F - Pinellas County Information Security Policy

In the event of an inconsistency in this Agreement and any of the attached Exhibits, the terms set forth in this Agreement will prevail.

**41. Entirety**

This Agreement constitutes the entire Agreement between the Parties and supersedes all prior negotiations, representations or agreements either oral or written.

**(Signature Page Follows)**

**AGREEMENT**

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement the day and year first written.

PINELLAS COUNTY, FLORIDA

By and through its County Commissioner

County Administrator

By

Charlie Justice, Chairman



Revere Control Systems Inc

Name of Firm

By:

Signature

Print Name

Title



Nan Johnson

VP of Municipal Systems

ATTEST: KEN BURKE, CLERK

By:



APPROVED AS TO FORM

By: Keiah Townsend

Office of the County Attorney

<b>AGREEMENT</b>
------------------

**EXHIBIT A - STATEMENT OF WORK****1.0 INTENT FOR INSTRUMENTATION CONTROL & MONITORING SYSTEMS REPAIR, MAINTENANCE, AND TRAINING.**

The intent of this Good and Services Agreement is to describe the minimum requirements necessary to provide for the provision of onsite technical assistance and training services to troubleshoot and repair all Instrumentation, Control, and Monitoring systems at various Pinellas County Utilities Water & Wastewater treatment facilities as specified in the table below.

**South Cross Bayou WRF:**

South Cross Bayou Water Reclamation Facility	7401 54 <sup>th</sup> Avenue, St Petersburg, FL
McKay Creek Repump Station	14800 118 <sup>th</sup> Avenue N Largo, FL
Pump Station 016	10548 Park Blvd, Seminole FL
Pump Station 054	1415 Indian Rocks Road, Largo, FL
St Pete Beach RCW Booster Station	7571 Boca Ciega Drive, St. Pete Beach, FL
Pump Station 163 Madeira Beach	150th Avenue, Madeira Beach, FL
Belleair Pump Station	1075 Ponce De Leon Drive, Belleair, FL
Fat Oil Grease Pump Station	11500 28 <sup>th</sup> Street, St Petersburg, FL

**Keller WTP:**

Keller Water Treatment Facility	3655 Keller Circle Tarpon Springs, FL
Logan Station Pump Station	1620 Ridge Road Largo, FL
North Booster	27707 U.S. 19 Clearwater FL
Gulf Beach	4501 Gulf Blvd, St. Pete Beach, FL
Madeira	201 150 Avenue N., Madeira Beach, FL
Capri	12050 2 <sup>nd</sup> Street. E. Treasure Island, FL

**W.E. Dunn WRF**

W.E. Dunn Water Reclamation Facility	4111-Dunn Drive Palm Harbor, FL
Reclaimed Water Intertie	3100 Tampa Road, Oldsmar, FL

**2.0 SCOPE OF SERVICES**

<b>AGREEMENT</b>
------------------

The Contractor, will provide all labor, materials, parts, tools, and any and all equipment and personal protective equipment (PPE) to perform various services including, but not limited to, maintenance, repair, testing, modification, and installation, and training, with the intent of prolonging the service life of the systems.

*While many types of Instrumentation Control and Monitoring Systems the most widely used devices and equipment include, but is not limited to, those listed below:*

<b>Modicon PLCs</b>	<b>Schneider M580</b>	<b>PLC's</b>	<b>Allen Bradley PLC's</b>
<b>Schneider M340 PLCs</b>	<b>Hach instruments</b>	<b>Elpro type hardware</b>	<b>Square D</b>
<b>Chlorine analyzers</b>	<b>Swan Instruments</b>	<b>Wonderware Application Server</b>	<b>SQL programming</b>
<b>Maple Touch Screen panel displays</b>	<b>PH analyzers</b>	<b>ACP Thin Clients</b>	<b>Cellular Modems</b>
	<b>PC's</b>		

## JOB ESTIMATE

- 2.1.1 Since this is a time and material contract, the Contractor shall provide a detailed job estimate on each project with a not-to-exceed price which will be evaluated by PCU staff for reasonableness of cost prior to authorization and commencement of the work to be done. Cost estimates do not have to be exact; however, they should reflect a realistic dollar amount cost for the work requested. All estimates shall be itemized and based upon quoted labor costs, material and equipment costs less MSRP discounts and includes the location of the job and the name of the technician assigned to the job. The signature, title, and contact information of the person providing the estimate must be legible.
- 2.1.2 PCU may elect to obtain other quotes should the estimate exceed PCU's budget and expectation of reasonableness in the Contractor's cost estimate.
- 2.1.3 Contractor shall provide current Manufacturer's Suggested Retail Price (MSRP) lists via a DVD disc or thumb drive or hard copy at the start of the contract and provide an updated list at any time if there is a manufacturer's price change for any parts/materials associated with this contract to County designee, SCADA Manager.

### 3.0 AUTHORIZATION FOR WORK

As work is needed, the Contractor will receive a Standard Purchase Order (SPO) that references specific information that corresponds with a job estimate. The SPO shall be considered authorization to initiate the start of a job.

## 4.0 GENERAL



<b>AGREEMENT</b>
------------------

4.1 The Contractor shall provide, at a minimum, the following services per the requirements that follow:

- 4.1.1 All work covered under this contract shall be performed in accordance with Instrumentation, Systems and Automation Society of America and the Institute of Electrical and Electronic Engineering Standards.
- 4.1.2 Contractor shall use his own test equipment necessary for emergency repair services of the designated process control systems.
- 4.1.3 Contractor shall repair or replace failed Programmable Logic Control (PLC) hardware, PLC software and other instrumentation equipment or devices upon authorization in the form of a purchase order.
- 4.1.4 Contractor shall advise and recommend to the County designee, Supervisory Control and Data Acquisition (SCADA) Manager and respective Pinellas County Utilities facility manager, the availability of applicable hardware upgrades.
- 4.1.5 Contractor shall make the County designee, SCADA Manager, aware of any operational software upgrades which are available and provide installation and configuration services if requested by purchase order. (Pinellas County Utilities (PCU) may elect to provide the software).
- 4.1.6 Contractor shall provide services to add or modify the instrumentation, control and monitoring systems software at the applications level under the direction and with the assistance of the County's (SCADA) group. This would include configuration of the system for the addition of new PLC's as well as addition or modification of Input/Output points of existing hardware.
- 4.1.7 Contractor shall provide services to troubleshoot, and repair process instrumentation such as tank level transmitters, pressure transmitters, flow meters etc. as authorized in writing by the County designee. Instruments shall be calibrated to applicable Instrument Society of America Standards.
- 4.1.8 Contractor shall provide assistance to the PCU, when and as needed with proper authorization, with recovery of the Instrumentation, Control and Monitoring systems following outages due to computer hardware/software failures, PLC component /software failures, vandalism, floods etc.
- 4.1.9 Contractor shall provide the labor and technical expertise required to assist PCU with modifications to existing instrumentation, control, and monitoring systems. Services to include, but are not limited to, installation and startup of new PLCs, new process instrumentation such as tank level transmitters, pressure transmitters, flow meters, etc., new process monitors, modems, or other communication equipment.
- 4.2.0 All changes made to the existing instrumentation, control, and monitoring systems shall be documented. Wherever necessary the contractor shall update all blueprints written documentation, program, and hardware changes. The contractor shall provide an electronic copy in pdf file format as applicable, to the County's SCADA group and three hard copies to the respective facility manager.

<b>AGREEMENT</b>
------------------

- 4.2.1 Contractor shall provide a detailed written service report, itemizing all costs at no extra charge to County designee, SCADA Manager.

## **5.0 CONTRACTOR REQUIREMENTS**

- 5.1 The Contractor shall have applicable experience with comparable instrumentation, control and monitoring systems and provide additional reference documentation with bid to substantiate experience submitted. Bids received that are missing documentation will be deemed non-responsive.
- 5.2 The Contractor must have a local service center, within a two (2) hour driving radius of Pinellas County, with qualified field technicians capable of troubleshooting and repair of Instrumentation, Control and Monitoring systems.
- 5.3 Contractor shall not substitute previous qualified techs/programmers/engineers without prior approval from PCU designee, SCADA Manager or respective facility manager.

## **6.0 SIGN IN/SIGN OUT LOG**

The contractor shall be required to sign in and out in a Log Book provided by PCU upon commencement or termination of work.

## **7.0 METHOD OF PAYMENT**

Contractor will be paid on the basis of time and material computed at fixed labor cost and a fixed discount percentage off MSRP list as submitted with quote, Section F.

## **8.0 PERSONNEL**

Personnel used to complete the work specified herein shall have the proper training and factory certification which may include but is not limited to: Bureau Veritas Certification in accordance with ISO 9001, ISO 14001 and ISO 45001; Certified Scada Security Architect CSSA certification must be submitted with the bid. Contractor must be able to perform the Contract requirements, and shall be able to produce verification of proper training and factory certification upon request by the County. Pinellas County may halt the work performance of a service technician if there are reasons to believe that the service technician is not qualified to perform the activity. The County has the right to request a new service technician to perform the work prescribed under this contract.

<b>AGREEMENT</b>
------------------

**9.0 ACCESS CONTROL**

All persons must review, acknowledge receipt of by signing and returning page with bid submittal information and adhere to the Official Pinellas County Security Policy (Exhibit F).

**10.0 REPAIR SERVICE**

- 10.1 Contractor shall provide telephone and on-site software support to the County as part of the services provided.
- 10.2 Contractor shall provide a 24-hour emergency contact number for County personnel to use.
- 10.3 The contractor shall provide on-site training. (see Training Section 12.0 for details)
- 10.4 County service calls must be requested on a 24 hour per day, 7 days per week basis.
- 10.5 ~~Emergency Response must be responded to within two (2) hours and service initiated. The emergency will be determined by Pinellas County Representative initiating the call.~~
- 10.6 The contractor will respond to calls logged as non-emergency within eight (8) hours.

**11.0 BUSINESS HOURS**

- 11.1 Pinellas County's normal business hours are 7:00 am to 3:30 pm Monday through Friday. After-hours services will be from 3:31 pm through 6:59 am Monday through Friday and all weekends and County recognized holidays.

**11.1.1 HOLIDAY SCHEDULE**

The following days shall be recognized holidays for the purposes of this contract.

New Year's Day	January 1
Martin Luther King's Birthday	Third Monday in January
Memorial Day	Last Monday in May

<b>AGREEMENT</b>
------------------

Independence Day	July 4
Labor Day	First Monday in September
Veteran's Day	November 11
Thanksgiving Day	Fourth Thursday in November
	Friday after Thanksgiving
Christmas Day	December 25

- 11.2 All service, regular and special, shall be rendered at such times and in such a manner that minimizes interference with normal facility operations.

## 12.0 TRAINING

- 12.1 The contractor shall be able to provide formal classroom onsite training to the appointed staff once a year while this contract is in force. The assistance shall include general operation, programming of PLCs, as requested by the County, implementation of control and process automation equipment, alarm, and measurement strategies and logic to accomplish desired additional functionality, and other technical support requested by County staff (related to supported equipment). The contractor will provide training on equipment and manufacturer specified by Pinellas County staff.

- 12.2 The training shall be provided as per section 12.1 upon request by the County.

### 12.1 ADDITIONAL TRAINING REQUIREMENTS

- 12.1.1 Training sessions shall be carefully planned and conducted with adequate instructional materials. Instructors shall be qualified personnel. Pinellas County reserves the right to review and approve instructors based on their qualifications and background.
- 12.1.2. As new hardware, software, or process control upgrades become available, contractor will notify Pinellas County designee, and if approved, will perform such upgrades and provide the necessary training.
- 12.1.3. It is the responsibility of the contractor to contact the designated County site representatives for scheduling all on-site training activities. Pinellas County will require a minimum of two weeks advance notification to assure the availability of equipment and staff for training.

## 13.0 WARRANTY

All repairs and services shall be warranted for a minimum of twelve (12) months. Any unit, which has a subsequent failure within this time frame, shall be re-inspected and repaired at no charge to Pinellas County.



<b>AGREEMENT</b>
------------------

**14.0 REPAIR / REPLACEMENT PARTS**

As part of the scope of service, all repair or replacement parts supplied shall be new, first quality products meeting original equipment manufacturer (OEM) specifications. Any upgrade of original OEM equipment needed shall be evaluated at the time of repair.

**15.0 CONFINED SPACE LANGUAGE**

The contractor shall submit, at the pre-commencement meeting, proof of employees certified in OSHA Confined Space Standard 29 CFR 190.146 for performing work in Confined Space Areas.

- a. The Contractor will be working in an area determined by OSHA regulations as a confined space. All work shall be in compliance with applicable OSHA regulations.
- b. Two continuous oxygen deficiency and lower explosive limit monitors shall be provided by the Contractor for each tank undergoing cleaning. The monitors shall be in operation at all times. If one unit fails, work may continue on the tank for a sufficient period of time to obtain a replacement unit but not more than 24 hours. If both units fail, all work shall stop inside the tank.
- c. Provide blower-induced ventilation to meet the requirements of OSHA. The blowers shall be in operation at all times work is in progress inside the tank until the area no longer meets the criteria of a confined space. The contractor shall provide emergency air packs for the employees and inspectors
- d. Contractor is responsible for following all Federal, State, or Local Laws, Standards, and Regulations pertaining to the safety and health of their workers and shall be accountable for any violations of such. The contractor shall be solely responsible for identifying and abatement of workplace hazards and is responsible for identifying appropriate personal protective equipment (PPE), as well as providing such PPE to their workers. The contractor is responsible for any on-the-job injuries or illness of contract employees per Federal, State, or Local Laws, Standards, or Regulations. The contract is responsible for providing safety training to contract workers. The safety and health of contract workers are the sole responsibility of the Contractor.

**16.0 MATERIALS**

All materials purchased under this Agreement must be new, the latest model, first quality, and carry the manufacturer's standard warranty.

**17.0 CONFLICT MINERALS**

The Contractor has taken reasonable actions necessary for the Contractor to be in compliance in all material respects with the disclosure requirements of applicable U.S. federal securities laws related to Conflict Minerals. "Conflict Minerals" means (a) columbite-tantalite (coltan), cassiterite, gold, wolframite, or their derivatives, which are limited to tantalum, tin, and tungsten, unless the Secretary of State of the United States determines that

AGREEMENT
-----------

additional derivatives are financing conflict in the Democratic Republic of the Congo or a country that shares an internationally recognized border with the Democratic Republic of the Congo; and (b) any other mineral or its derivatives determined by the Secretary of State of the United States to be financing conflict in the Democratic Republic of the Congo or a country that shares an internationally recognized border with the Democratic Republic of the Congo.

## 18.0 BACKGROUND CHECKS

### SECURITY AND BACKGROUND CHECKS

All Contractor employees are required to submit to a background check. The background check process shall be completed at least ten (10) days prior to the start of the contract. The Contractor shall be responsible for all costs associated with the background checks. A valid driver's license and Social Security card are required for completing the background check and obtaining a security clearance. Orientation for the Security Clearance workflow process will be provided to the awardee.

**Step One** – The Contractor shall obtain a Level One Criminal History Records Check through the Florida Department of Law Enforcement (FDLE) for each assigned employee.

**Step Two** – The Contractor shall submit the FDLE Records Check along with a copy of the driver's license, Social Security card, and completed Sheriff's Office Security Clearance Application, for each employee, to the Facility Operations support team.

The Pinellas County Sheriff's Office shall have and exercise full and complete control over granting, denying, withholding, withdrawing, or terminating security clearances for contractor employees. **If a submitted employee is denied for any reason, there is no opportunity to re-apply.**

**Additional Requirements for areas with confidential law enforcement documents and data:** The Contractor shall submit for fingerprinting all personnel working in any area deemed confidential. The Contractor will schedule through the Facility Operations Support team a time for

the employees to be fingerprinted by the Sheriff's Office. All personnel that has successfully completed fingerprinting are required to complete online Security and Awareness training.

Additional Requirements exist for the Young-Rainey STAR Center facilities. If applicable, the Contractor will submit to the County representative the following:

- Original birth certificate
- Original passport (proof that subject is a naturalized citizen of the United States of America)

**AGREEMENT**

No copies will be accepted. The Contractor will schedule through the Facility Manager a time for his employees to present their documents to the County representative.

The Contractor is responsible to pay for this added clearance requirement. The County representative shall have and exercise full and complete control over granting, denying, withholding, with-drawing, or terminating security clearances for contractor employees for the County locations only.

**Step Three** - The Facility Operations Support team will communicate the results of the Sheriff's Office review to the Contractor.

- a) A list of all assigned personnel, showing the employee's full name, address, telephone number, date, and place of birth, and driver's license or State ID number, and their assigned work location shall be submitted to the Facility Operations support team. This list is to be kept current by the Contractor and promptly submitted to the Facility Operations Support team at the beginning of each month. This referenced document is called the Employee Assignment Sheet (EAS). The EAS template will be provided to the awardee.
- b) The Contractor shall provide an updated FDLE Level One Criminal History Records Check for all personnel on an annual basis. The annual updates are to be sent to the Facility Operations support team for review by the Sheriff's Office. Background check updates shall remain on file at the Contractor's location for three (3) years from the date of the last invoice.
- c) All Contractor employees are required to wear identification (ID) badges, to be furnished by Pinellas County for the various facility sections. The Contractor shall make the employees available for photographs on a schedule to be worked out with the Facility Manager. Access to sites not managed by the Real Estate Management Department needs to be coordinated with the County site representative for the specific department. The badges shall be made by the County before an individual may begin work and only after a favorable security clearance has been received. Contractor employees shall sign each badge at the time of receipt.
- d) The Contractor will notify the respective Facility Manager when an employee badge is lost. It shall be the responsibility of the contractor to pay for replacement badges at the rate of \$10.00 per badge. No employee shall be allowed to work without a current badge. Any contract employee who does not have proper identification shall be cause for the County to require removal of that employee from the property. The Contractor shall see that all badges are returned to the Facility Manager when employees are dismissed or terminated.

**19.0 CYBER SECURITY LANGUAGE**

The Contractor and each of its subsidiaries have taken all technical and organizational measures necessary to protect the information technology systems and data used in connection with the operation of the Contractor's and its subsidiaries' businesses. Without limiting the foregoing, the Contractor and its subsidiaries have used reasonable efforts to establish and maintain, and have established, maintained, implemented, and complied with, reasonable information technology, information security, cyber security, and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent a breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or Data used in connection with the operation of the

**AGREEMENT**

Contractor's and its subsidiaries' businesses ("Breach"). There has been no such Breach, and the Contractor and its subsidiaries have not been notified of and have no knowledge of any event or condition that would reasonably be expected to result in, any such Breach. The continuous functionality and threat protection of the Pinellas County Utility (PCU) SCADA System is critical. The contractor must comply with all PCU Cyber and Information Security policies and procedures. In the absence of specific guidance, users should contact the PCU SCADA Department for recommendations. Policy violations may result in a temporary or permanent loss of system access. Requirements include but are not limited to:

**a. SCADA Secure Laptops**

- i. Both onsite and offsite SCADA work requiring network or device connectivity is restricted to specially configured laptops or computers provided by PCU. These laptops may not be used for any other purpose, including internet and email access.
- ii. Network access by unauthorized personal or contractor business devices, including laptops, PCs, cell phones, and tablets, is strictly prohibited.

**b. Connection Requirements**

- i. SCADA will coordinate with the Pinellas County IT Department (BTS) to establish a Virtual Private Network (VPN) connection for each user requiring access. Shared accounts or login information is banned.
- ii. SCADA servers utilize Multifactor Authentication (MFA) which involves the use of cell phones and/or security dongles.

**c. Remote Access – Remote access is reserved for special circumstances, must be approved by the SCADA Department and Plant Operations, and is subject to additional restrictions.**

- i. Access is limited to SCADA Secure Laptops through a PCU VPN.
- ii. Planned Access - The contractor must notify SCADA in advance regarding scheduled remote access. Remote hours may be restricted to PCU standard business hours to ensure County staff is available to monitor and support the engagement.
- iii. Unplanned Access – The contractor must notify and receive approval from SCADA before connecting to the network. After-hours access should be limited to startup or requested downtime troubleshooting.
- iv. File transfers are limited to approved methods and may require the assistance of the SCADA Department. USB storage drives and unauthorized device connections to SCADA Secure Laptops are prohibited.

**d. Network and HMI Application Restrictions – Access to select SCADA resources or control functions may be limited or require special permission.**

## **20.0 STANDARDS**

All work shall conform to established or evident department standards for system configuration, documentation, PLC logic, graphical interface, tag/object naming, data collection, and scripting. Deviations or exceptions will require County approval.

## **21.0 PLACE OF SERVICE**

The contractor, in the performance of all services under this Agreement, may require its property and/or employees, subcontractors, consultants or, other agents to go upon County's property and to be in proximity of County's employees and contractors. The contractor agrees that in doing so, proper precautions will be taken to carry on its operations in a safe, competent, and professional manner at all times, both in performing the services under this Agreement and in entering and leaving County's property. Neither Contractor nor its employees, subcontractors, consultants, or other agents shall permit or enable any unnecessary person to enter County's premises, nor permit or enable to enter County's premises any person County has requested be removed from and precluded from

**AGREEMENT**

entering County's premises, whether for reasons of security of persons, property or information. The contractor shall require its employees, subcontractors, consultants, and other agents to comply with the policies and procedures made known by the County concerning entry, exit, and conduct upon the County's premises, including background screening and use of security badges or access cards if required by County. The contractor shall not permit any person to obtain or retain possession of any access card or device beyond the conclusion of the Work or otherwise beyond the duration of the County's express authorization. The contractor shall obtain appropriate background checks on all of the Contractor's employees, agents, or consultants prior to their entry on Pinellas County premises, and will ensure all subcontractors are held to the same standard relating to their employees, agents, or consultants performing services on County premises.

In all instances, Contractor shall honor requests for immediate removal of Contractor's employees, sub-contractors, consultants, agents, etc. in instances deemed to involve a conflict of interest, or for any other reason(s) deemed to be in County's best interest, at County's sole reasonable discretion.

**22.0 COVID LANGUAGE**

The contractor agrees to follow the then-current State Department of Health and CDC guidelines concerning COVID. If a Contractor, their employees, consultants, delivery drivers, or representatives becomes sick (symptoms may include fever, cough, and shortness of breath) the Contractor will ensure that said person will not provide services until verification of testing negative for COVID has been conducted.

Contractors that experience delays on projects due to COVID-19 should rely on the following best practices to request/claim excusable time extensions and avoid government terminations. Contractors shall provide timely notice and Contractor shall keep performing when possible.

**23.0 PINELLAS COUNTY'S COMPUTER USAGE POLICY**

In all instances when Contractors are using or connecting to Pinellas County computer systems, it is the expectation of Pinellas County that the highest level of discretion and caution be used in ensuring the security of Pinellas County's systems.

In addition, when using or connecting to any Pinellas County systems, it is Pinellas County's expectation that good judgment and professionalism be used as relates to email and/or internet activity in order to ensure all Pinellas County systems are utilized in a legal and ethical manner.

Further, it is Pinellas County's expectation that all Pinellas County systems be used solely for the purpose authorized and intended based upon the nature of services being provided to Pinellas County by the Contractor.

The above applies to all Contractors using or accessing Pinellas County computers, including those that may be using privately owned computers or systems to access Pinellas County systems resources. Pinellas County systems resources include any computers, workstations, hand-held computing devices, servers, and networks

<b>AGREEMENT</b>
------------------

provided or supported by Pinellas County and the information, software programs, and utilities stored on or created by them.

Any violation of the above may be viewed as a breach of Agreement at the sole discretion of Pinellas County.

#### **24.0 ASSIGNMENT**

Neither party may assign this Agreement, in whole or in part, without the express written consent of the other party. This Agreement shall bind all assigns and successors.

#### **25.0 EQUAL OPPORTUNITY / GIFT & GRATUITY POLICY**

Pinellas County is committed to a workplace, which is free from harassment or discrimination of any kind. All Contractors and their agents, while performing work and/or services pursuant to this Agreement, are expected to conduct themselves accordingly.

All employees of Pinellas County are prohibited from accepting gifts and/or gratuities from Contractors. The contractor agrees to cause all of its employees, subcontractors, consultants, and other agents to honor this policy.

#### **26.0 SUPERVISION**

The contractor shall supply supervision for all employees working on site. The contractor's employees shall not operate any Pinellas County equipment, including but not limited to telephones, fax machines, televisions, microwaves, or computers.

#### **27.0 GOODWILL**

The contractor understands and agrees that Pinellas County has substantial investments to create and protect its image, reputation, and goodwill in the communities it serves and that such image, reputation, and goodwill are significant, highly valuable assets. Accordingly, Contractor, its employees, and representatives will exercise due diligence to avoid any injury or interference with Pinellas County's goodwill and will not, through act or omission, injure or negatively interfere with its image, reputation, or goodwill with customers or other members of the communities it serves. Any such injury or interference is a material breach of this Agreement and grounds for immediate termination without further obligation on the part of Pinellas County to Contractor except amounts owed for previous services rendered.

#### **28.0 COUNTY REQUIREMENTS**



**AGREEMENT**

- 15.1 The County will provide its own personnel to perform equipment calibrations except in unusual situations when the contractor's service may be necessary.
- 15.2 If there are questions when a repair call is considered an emergency, the County's Site Supervisor will make the decision as to whether the call is an emergency or not. The "Emergency" shall refer to a critical equipment or process downtime scenario that requires an immediate response. Response procedures shall be discussed at the time of the "call-out". In the absence of any documentation, the facilities may have for site entry or conduct. Contractors shall remain in contact with the incident representative and be prepared to follow instructions related to any Emergency circumstance that may arise.

**GROUP TWO - INTENT FOR ONSITE/OFFSITE CONSULTING**
**1.0 CONTRACTOR REQUIREMENTS:**

- a. The Contractor is responsible for fulfilling County's staffing requests with qualified personnel within the time frames required by the County for the job classifications included herein.
- b. The contractor shall provide labor and technical expertise to assist the Pinellas County Utilities (PCU) SCADA Department with installation, configuration, troubleshooting, and documentation of the PCU SCADA system. Projects and tasks will be defined as needed by PCU SCADA and completed under their supervision. Requirements may dictate work be performed onsite at PCU facilities and/or through remote VPN connection when approved, using only authorized cyber secure devices and procedures.
- c. Assigned personnel should have advanced knowledge and experience with Aveva Industrial Automation software.
  - i. System Platform
  - ii. Intouch for System Platform
  - iii. Historian
  - iv. Historian Client
  - v. I/O Servers & System Management Console
- d. The contractor should also have basic concept knowledge with the following auxiliary software/systems and be prepared to assist the PCU SCADA department with guidance.
  - i. Microsoft Windows and Server Software
  - ii. Microsoft Windows Server Update Services
  - iii. Microsoft Remote Desktop applications
  - iv. Virtual Machines
  - v. Microsoft SQL Server
  - vi. General networking principles
  - vii. Rockwell ThinManager for thin clients
  - viii. Pump Station Operations
  - ix. Cellular modems and communication
  - x. Motorola PLCs and programming software
  - xi. DNP3 communication protocol
  - xii. Schneider PLCs and programming software
  - xiii. Physical Security System components
- e. The Contractor will be responsible for ensuring that all personnel assigned are qualified to perform the functions and duties specified in the County's request. Only technicians/programmers who have passed the

## AGREEMENT

Aveva Certified System Integrator Exam for Application Server (2017 or 2020) will be accepted. Alternatively, those with 2 years of documented project experience with System Platform (Application Server) and InTouch for System Platform may be considered subject to screening. PCU SCADA reserves the right to request a replacement for unqualified or underperforming programmers. Contactor shall at minimum conduct all employment screening, testing, evaluations, and recruitments necessary to assess personnel qualifications, as more fully set forth below or in a County request document. All pre-placement screening is to be compliant with applicable federal, state, and local laws including but not limited to Title VII of the Civil Rights Act of 1964, as amended, Fair Credit Reporting Act (FCRA), and the Genetic Information Nondiscrimination Act.

- f. Additionally, with respect to required screenings and criminal background checks, Contactor will comply in all respects with the requirements stated in Fla. Stat. 435.04.
- g. After a complete and satisfactory pre-placement screening has been conducted, a Onsite/Offsite Contractor will be submitted to the hiring manager identified in the request.
- h. Employment Screening, Testing, Evaluations, Recruiting:

In order to identify and place Onsite/Offsite Contractors responsive to a County request, Contactor will, at a minimum:

- i. Match job descriptions to job resumes
- ii. Match skills and competencies to the required job level
- iii. Conduct phone interview
- iv. Complete preliminary assessment (in person, structured panel interviews and/or video)
- v. Ensure Onsite/Offsite Contractor completes pre-employment testing
- vi. Complete verification of the Onsite/Offsite Contractor via prior employment/reference check, education, criminal background check, MVR history, 5- Panel drug and alcohol testing, work eligibility
- vii. Personnel Protective Equipment (PPE): qualified contractor personnel will arrive on the job with all required standard safety equipment, at no additional cost to the County: leather palm work gloves, safety glasses, hard hat, earplug/muffs, and steel-toed boots.
- viii. Safety Training Program: Contactor will regularly conduct safety training programs using videos and handouts for a variety of subjects, including Hazardous Communications.
- i. Employment History. Check

Before a Onsite/Offsite Contractor is placed at the County under this contract, Contactor will confirm Onsite/Offsite Contractor's previous employment history via an interview with a previous supervisor who worked directly with the Onsite/Offsite Contractor to identify past performance and any problems that came about during the Onsite/Offsite Contractor's employment. Contactor will also verify job duties, performance evaluations, strengths and weaknesses, and acceptable attendance records.

- j. Education Verification

Before an Onsite/Offsite Contractor is placed at the County under this contract in a specific professional and technical position, Contactor will complete education verification using National Student Clearinghouse to verify education background. Contactor will identify Onsite/Offsite Contractor's degree/diploma/credential, graduation or completion date, major of degree, official educational accrediting body.

<b>AGREEMENT</b>
------------------

k. Criminal Background Check

Contractor will conduct nationwide background checks including but not limited to criminal history, employment, motor vehicle history, including Florida Department of Law Enforcement (FDLE) reporting. County will specify the background result standards that shall be applied in each County request for an assigned Contractor Personnel, and no person shall be assigned as a Contractor Personnel if their screening results do not meet the standards specified.

Background checklist will include:

- i. Complete background checks ten prior to the start of an assignment, and the completed background check should not be older than twelve (12) months at the time of the start of an assignment. Contractor will also promptly notify County if Contractor becomes aware of additional background information or new information related to the standards of the background check that develop after the start of the assignment.
- ii. Background check results shall remain on file at Contractor for three (3) years from the date of the last invoice.
- iii. Contractor will provide County with a list of all assigned Contractor Personnel.

l. 5-Panel Drug and Alcohol Testing

The County is a drug-free workplace, and the Contractor recognizes County as a drug-free workplace. The contractor will conduct drug and alcohol testing through a 5-Panel drug test and alcohol test for each Onsite/Offsite Contractor prior to placement and conduct annual follow-up checks. Drug and alcohol test results should not be older than twelve (12) months at the start of an assignment. The contractor will not place or will replace any individual with a positive result on a drug and alcohol test.

m. Work Eligibility

Immigration Reform and Control Act: Contractor will verify that each contractor personnel assigned under this contract is eligible to work in conformance with the Immigration Reform and Control Act of 1986 located at 8 U.S.C. 1324, et. Seq., and regulations relating thereto, as may be amended from time to time, and the Illegal Immigration Reform and Immigration Responsibility Act of 1996. Failure of Contractor to comply will be deemed a material breach and shall be cause for immediate termination of the contract at the discretion of the County.

n. Motor Vehicle Driving Requirements

Contractor will review the Florida (or appropriate state) driver's license history record for the last four (4) years. Contractor personnel with unacceptable driving records will not be placed in positions requiring driving. Unacceptable driving records include any of the following:

## AGREEMENT

- i. Any citation for DUI, or refusal to be tested for DUI, regardless of a conviction, a plea of guilty, or no contest plea;
  - ii. Any conviction for reckless or careless driving in the preceding three (3) years;
  - iii. Suspension or revocation of the driver's license in the preceding four (4) years. Suspension for failure to maintain PIP and comply with Child Support requirements are excluded from this suspension provision; if the suspension has been concluded;
  - iv. Two (2) or more moving violation convictions in the preceding three (3) years;
  - v. A business purpose exemption or inter-lock device restriction in place. The record must be cleared before staff can drive a County vehicle.
  - vi. County will not be responsible for driver training, but placed staff will attend the County's driver safety training when required. Contractor personnel will only be allowed to operate Class E Level vehicles/non-commercial vehicles. Those hired for driving positions will not be allowed to drive a commercial vehicle regardless of having a CDL license.
- o. Contractor's Compensation or its Employees and Compliance with Laws
- i. Contactor will be responsible for payment to its employees including all payroll reporting including the withholding of income and payroll taxes. Contactor's costs for any and all such requirements and/or the provision of any employee benefits it provides to its staff is its sole responsibility and the County will not increase billing rates hereunder to cover such costs. No additional costs will be passed through or separately billed to the County to cover any tax, or benefit obligations of Contactor to its employees.
  - ii. Contactor is responsible for full compliance with all federal, state, and local laws relating to the employment of persons, including but not limited to, the fair Labor Standards Act, the Family & Medical Leave Act, the Americans with Disabilities Act, and the Affordable Care Act, Title VII of the Civil Rights Act of 1964, as amended and Florida's Worker's Compensation Law.
  - iii. Contactor may at times maintain a physical office in Pinellas County and shall not be entitled to use any County facility except upon prior agreement of the parties.
- p. Transition  
Contactor is solely responsible for filling all currently filled positions as of the start of the contract.
- q. COUNTY REQUIREMENTS:
- i. The County will provide worksite location information, Utilities SCADA and Security Systems Manager's name, and relevant contact details
  - ii. Reason for request, expected duration, work schedule, start and end dates
  - iii. Position title, duties, knowledge, skills, and certifications
  - iv. Contractor attire and equipment (business, business casual, uniform, other)
  - v. Required work-related equipment or PPE
  - vi. Sensitive assignment and/or interaction with the public, children, disabled persons, cash/credit card transactions, location background check (airport, sheriff's department)
  - vii. Background and screening results standards to be applied
- r. BUILDING SECURITY AND ACCESS CONTROL

All contractor personnel are required to wear picture identification badges, to be furnished by Pinellas County, while at County's various locations. Any keys or key cards issued to Contactor for such use will not be duplicated by Contactor or contractor personnel. Contactor will make contractor personnel available for photographs on a schedule to be determined with the County's Human Resources Department.

**AGREEMENT**

- i. Badges will be made by the County prior to individual beginning work. Each contractor personnel shall sign his or her badge at the time of receipt.
  - II. Contactor will notify Human Resources when a badge is lost.
  - III. Contactor will pay to County \$10.00 per badge for any replacement badges.
  - IV. No Contractor Personnel will be allowed to work without a current badge. Contractor Personnel who do not display proper identification will give cause for the County to require removal of that individual from the property.
  - V. Contactor will see that all badges are returned to County when an individual is no longer assigned under the contract.
  - VI. Contactor has been notified that for security purposes, all Pinellas County properties may be under video surveillance, and shall communicate this to all Contractor Personnel. The County will not be responsible for any loss of personal property by Contactor or contractor personnel placed with the County.
  - VII. No parking will be provided for Contractor Personnel assigned to work at the County.
- s. **REMOVAL OF TEMPORARY STAFF**
- County will be provided a 24-hour contact number to handle issues if/when they arise. Contactor will remove a temporary staff from an assignment upon the County's request. Temporary staff will be escorted from the County's property as required. County will not be charged for staff incapable of performing a job assignment. The following are examples of unacceptable behaviors of Contactor temporary staff, but are not all-inclusive:
- i. Violation of safety rules, and/or misuse of County's property
  - ii. Use of alcohol or controlled substances while on duty
  - iii. Unreliable attendance
  - iv. Insubordination. Contractor personnel are expected to take direction from the County's department supervisor/manager and behave in a manner deemed appropriate and respectful.
  - v. Disrupting the work environment. Non-cooperation with co-workers will not be tolerated.
- t. **REPORTING**
- i. Contactor will provide monthly and quarterly reporting of usage identified by the Utilities SCADA and Security Systems Manager, with the ability to determine usage within each department. Responses must include at a minimum Contractor Personnel name, start date, pay rate. The number of hours worked per week, position title, location, hiring manager name and phone number as well as any other information relevant to the assignment requested by the County.
  - ii. Contactor will provide to County a monthly spend report that details each Utilities SCADA and Security Systems Manager's contractor personnel usage. In addition to monthly reports, Contactor will also provide additional reports upon request by County.
  - iii. All reporting shall be customizable to meet the needs of the County.
  - iv. Contactor is responsible for time reporting and shall monitor a variety of reports daily, reviewing and verifying contractor personnel work hours, scheduling, approving time off requests, monitoring attendance and vacancies.

<b>AGREEMENT</b>
------------------

**EXHIBIT B - INSURANCE REQUIREMENTS****1. LIMITATIONS ON LIABILITY**

By submitting a Bid, the Vendor acknowledges and agrees that the services will be provided without any limitation on the Vendor's liability. The County objects to and shall not be bound by any term or provision that purports to limit the Vendor's liability to any specified amount in the performance of the services. The Vendor shall state any exceptions to this provision in its response, including specifying the proposed limits of liability in the stated exception to be included in the Services Agreement. The Vendor is deemed to have accepted and agreed to provide the services without any limitation on the Vendor's liability that the Vendor does not take exception to in its response. Notwithstanding any exceptions by the Vendor, the County reserves the right to declare its prohibition on any limitation on the Vendor's liability as non-negotiable, to disqualify any Bid that includes exceptions to this prohibition on any limitation on the Vendor's liability, and to proceed with another responsive, responsible proposal, as determined by the County in its sole discretion.

**2. INDEMNIFICATION**

Vendor agrees to indemnify, pay the cost of defense, including attorney's fees, and hold harmless the County, its officers, employees and agents from all damages, suits, actions or claims, including reasonable attorney's fees incurred by the County, of any character brought on account of any injuries or damages received or sustained by any person, persons, or property, or in any way relating to or arising from the Agreement; or on account of any act or omission, neglect or misconduct of Contractor; or by, or on account of, any claim or amounts recovered under the Workers' Compensation Law; or of any other laws, regulations, ordinance, order or decree; or arising from or by reason of any actual or claimed trademark, patent or copyright infringement or litigation based thereon; or for any violation of requirements of the Americans with Disabilities Act of 1990, as may be amended, and all rules and regulations issued pursuant thereto (collectively the "ADA") except when such injury, damage, or violation was caused by the sole negligence of the County.

**3. INSURANCE**

The Vendor must provide a certificate of insurance and endorsement in accordance with the insurance requirements listed below, prior to recommendation for award.

The Vendor shall obtain and maintain and require any subcontractor to obtain and maintain, at all times during its performance of the Agreement, insurance of the types and in the amounts set forth. For projects with a Completed Operations exposure, Vendor shall maintain coverage and provide evidence of insurance for two (2) years beyond final acceptance. All insurance policies shall be from responsible companies duly authorized to do business in the State of Florida and have an AM Best rating of A- VIII or better.

- A. Submittals should include, the Vendor's current Certificate(s) of Insurance. If Vendor does not currently meet insurance requirements, Vendor shall also include verification from their broker or agent that any required insurance not provided at that time of submittal will be in place prior to the award of contract.

Upon selection of Vendor for award, the selected Vendor shall email certificate that is compliant with the insurance requirements. If the certificate received is compliant, no further action may be necessary. The Certificate(s) of Insurance shall be signed by authorized representatives of the insurance companies shown on the Certificate(s). **The Certificate holder section shall indicate Pinellas County, a Subdivision of the State of Florida, 400 S Fort Harrison Ave, Clearwater, FL 33756. Pinellas County shall be named as an Additional Insured for General Liability. A Waiver of Subrogation for Workers Compensation shall be provided if Workers Compensation coverage is a requirement.**

- B. Approval by the County of any Certificate(s) of Insurance does not constitute verification by the County that the insurance requirements have been satisfied or that the insurance policy shown on the Certificate(s) of Insurance is in compliance with the requirements of the Agreement. County reserves the right to require a certified copy of the entire insurance policy, including endorsement(s), at any time during the Bid and/or contract period.

- C. If any insurance provided pursuant to the Agreement expires or cancels prior to the completion of the



<b>AGREEMENT</b>
------------------

Work, you will be notified by CTrax, the authorized vendor of Pinellas County. Upon notification, renewal Certificate(s) of Insurance and endorsement(s) shall be furnished to Pinellas County Risk Management at [InsuranceCerts@pinellascounty.org](mailto:InsuranceCerts@pinellascounty.org) and to CTrax c/o JDi Data at [PinellasSupport@ididata.com](mailto:PinellasSupport@ididata.com) by the Vendor or their agent prior to the expiration date.

- 1) Vendor shall also notify County within twenty-four (24) hours after receipt, of any notices of expiration, cancellation, nonrenewal or adverse material change in coverage received by said Vendor from its insurer Notice shall be given by email to Pinellas County Risk Management at [InsuranceCerts@pinellascounty.org](mailto:InsuranceCerts@pinellascounty.org). Nothing contained herein shall absolve Vendor of this requirement to provide notice.
- 2) Should the Vendor, at any time, not maintain the insurance coverages required herein, the County may terminate the Agreement.

D. If subcontracting is allowed under this Bid, the Primary Vendor shall obtain and maintain, at all times during its performance of the Agreement, insurance of the types and in the amounts set forth; and require any subcontractors to obtain and maintain, at all times during its performance of the Agreement, insurance limits as it may apply to the portion of the Work performed by the subcontractor; but in no event will the insurance limits be less than \$500,000 for Workers' Compensation/Employers' Liability, and \$1,000,000 for General Liability and Auto Liability if required below.

All subcontracts between the Vendor and its Subcontractors shall be in writing and are subject to the County's prior written approval. Further, all subcontracts shall

1. Require each Subcontractor to be bound to the Vendor to the same extent the Vendor is bound to the County by the terms of the Contract Documents, as those terms may apply to the portion of the Work to be performed by the Subcontractor;
2. Provide for the assignment of the subcontracts from the Vendor to the County at the election of Owner upon termination of the Contract;
3. Provide that County will be an additional indemnified party of the subcontract;
4. Provide that the County will be an additional insured on all insurance policies required to be provided by the Subcontractor except workers compensation and professional liability;
5. Provide a waiver of subrogation in favor of the County and other insurance terms and/or conditions
6. Assign all warranties directly to the County; and
7. Identify the County as an intended third-party beneficiary of the subcontract. The Vendor shall make available to each proposed Subcontractor, prior to the execution of the subcontract, copies of the Contract Documents to which the Subcontractor will be bound by this Section C and identify to the Subcontractor any terms and conditions of the proposed subcontract which may be at variance with the Contract Documents.

E. Each insurance policy and/or certificate shall include the following terms and/or conditions:

- 1) The Named Insured on the Certificate of Insurance and insurance policy must match the entity's name that responded to the solicitation and/or is signing the agreement with the County.
- 2) Companies issuing the insurance policy, or policies, shall have no recourse against County for payment of premiums or assessments for any deductibles which all are at the sole responsibility and risk of Vendor.
- 3) The term "County" or "Pinellas County" shall include all Authorities, Boards, Bureaus, Commissions, Divisions, Departments and Constitutional offices of County and individual members, employees thereof in their official capacities, and/or while acting on behalf of Pinellas County.
- 4) All policies shall be written on a primary, non-contributory basis.

<b>AGREEMENT</b>
------------------

The minimum insurance requirements and limits for this Agreement, which shall remain in effect throughout its duration and for two (2) years beyond final acceptance for projects with a Completed Operations exposure, are as follows:

- 1) **Workers' Compensation Insurance:** Worker's Compensation Insurance is required if required pursuant to Florida law. If, pursuant to Florida law, Worker's Compensation Insurance is required, employer's liability, also known as Worker's Compensation Part B, is also required in the amounts set forth herein

Limits	Florida Statutory
<b>Employers' Liability Limits</b>	
Per Employee	\$ 500,000
Per Employee Disease	\$ 500,000
Policy Limit Disease	\$ 500,000

If Vendor/Contractor is not required by Florida law, to carry Workers Compensation Insurance in order to perform the requirements of this Agreement, County Waiver Form for workers compensation must be executed, submitted, and accepted by Risk Management. Failure to obtain required Worker's Compensation Insurance without submitting and receiving a waiver from Risk Management constitutes a material breach of this Agreement.

- 2) **Commercial General Liability Insurance:** including, but not limited to, Independent Vendor, Contractual Liability Premises/Operations, Products/Completed Operations, and Personal Injury.

<b>Limits</b>	
Combined Single Limit Per Occurrence	\$ 1,000,000
Products/Completed Operations Aggregate	\$ 2,000,000
Personal Injury and Advertising Injury	\$ 1,000,000
General Aggregate	\$ 2,000,000

- 3) **Excess or Umbrella Liability Insurance** excess of the primary coverage required, in paragraphs (1) and (2) above:

<b>Limits</b>	
Each Occurrence	\$1,000,000
General Aggregate	\$1,000,000

- 4) **Cyber Risk Liability (Network Security/Privacy Liability) Insurance** including cloud computing and mobile devices, for protection of private or confidential information whether electronic or non-electronic, network security and privacy; privacy against liability for system attacks, digital asset loss, denial or loss of service, introduction, implantation or spread of malicious software code, security breach, unauthorized access and use; including regulatory action expenses; and notification and credit monitoring expenses with at least minimum limits as follows:

<b>Limits</b>	
Each Occurrence	\$3,000,000
General Aggregate	\$3,000,000

<b>AGREEMENT</b>
------------------

For acceptance of Cyber Risk Liability coverage included within another policy required herein, a statement notifying the certificate holder must be included on the certificate of insurance and the total amount of said coverage per occurrence must be greater than or equal to the amount of Cyber Risk Liability and other coverage combined.

- 5) **Property Insurance** Vendor will be responsible for all damage to its own property, equipment and/or materials.

<b>AGREEMENT</b>
------------------

**EXHIBIT C - PAYMENT SCHEDULE**

<b><u>Group 1</u></b>		<b>VENDOR: Revere Control Systems Inc</b>			
<b><u>Item No.</u></b>	<b><u>Description</u></b>	<b><u>Quantity for a five-year period</u></b>	<b><u>Unit of Measure</u></b>	<b><u>Fixed Unit Rate</u></b>	<b><u>Extended Cost</u></b>
1	Training Conducted by Contractor Normal Working Hours 7:00 am – 3:30 pm Mon thru Fri	80	Hour	\$ 125.00	\$ 10,000.00
2	Training Conducted by Contractor Normal Working Hours 7:00 am – 3:30 pm Mon thru Fri	10	Day (8 Hours)	\$ 1,000.00	\$ 10,000.00
3	Service / Repair Technician Normal Working Hours 7:00 am – 3:30 pm Mon thru Fri	700	Hour	\$ 112.00	\$ 78,400.00
4	Engineer Normal Working Hours 7:00 am – 3:30 pm Mon thru Fri	200	Hour	\$ 125.00	\$ 25,000.00
5	Calibration Normal Working Hours 7:00 am – 3:30 pm Mon thru Fri	200	Hour	\$ 112.00	\$ 22,400.00
6	Programming Normal Working Hours 7:00 am – 3:30 pm Mon thru Fri	500	Hour	\$ 125.00	\$ 62,500.00
7	Panel Fabrication/ Construction Normal Working Hours 7:00 am – 3:30 pm Mon thru Fri	100	Hour	\$ 78.00	\$ 7,800.00
8	Programmable Logic Controller (PLC) Programmer Normal Working Hours 7:00 am – 3:30 pm Mon thru Fri	100	Hour	\$ 125.00	\$ 12,500.00
9	Service/Repair Technician Emergency Services After Hours 3:31 pm – 6:59 am Mon thru Fri Weekends/Holidays	20	Hour	\$ 168.00	\$ 3,360.00

<b>AGREEMENT</b>
------------------

10	Engineer Emergency Services After Hours 3:31 pm – 6:59 am Mon thru Fri Weekends/Holidays	20	Hour	\$ 187.50	\$ 3,750.00
11	Calibration Emergency Services After Hours 3:31 pm – 6:59 am Mon thru Fri Weekends/Holidays	20	Hour	\$ 168.00	\$ 3,360.00
12	Programming Emergency Services After Hours 3:31 pm – 6:59 am Mon thru Fri Weekends/Holidays	20	Hour	\$ 187.50	\$ 3,750.00
13	Panel Fabrication/ Construction Emergency Services After Hours 3:31 pm – 6:59 am Mon thru Fri Weekends/Holidays	20	Hour	\$ 117.00	\$ 2,340.00
14	Programmable Logic Controller (PLC) Programmer Emergency Services After Hours 3:31 pm – 6:59 am Mon thru Fri Weekends/Holidays	20	Hour	\$ 187.50	\$ 3,750.00
<b>Group 1 Subtotal</b>					<b>\$ 248,910.00</b>

<b><u>Group 2</u></b>					
<b><u>Item No.</u></b>	<b><u>Description</u></b>	<b><u>Quantity for a five-year period</u></b>	<b><u>Unit of Measure</u></b>	<b><u>Fixed Unit Rate</u></b>	<b><u>Extended Cost</u></b>
16	SCADA Support Programmer Normal Working Hours 7:00 am – 3:30 pm Mon thru Fri	4500	Hour	\$ 125.00	\$ 562,500.00
<b>Group 2 Subtotal</b>					<b>\$ 562,500.00</b>

<b>AGREEMENT</b>
------------------

<u>Item No.</u>	<u>Description</u>	<u>Quantity</u>	<u>Expenditure</u>	<u>% Discount</u>	
15	<b>Unspecified Parts As Needed</b> - Orders for unspecified parts is defined as like materials that may be required due to unexpected conditions or events. Unspecified Parts is <b>Not Guaranteed</b> as part of the contract and must be properly authorized by the County before delivery.	Dollars	\$25,000.00	0%	\$ 25,000.00
<b>Unspecified Subtotal</b>					\$ 25,000.00

<b>Grand Total</b>	<b>\$ 836,410.00</b>
--------------------	----------------------



<b>AGREEMENT</b>
------------------

**EXHIBIT D - PAYMENT/INVOICES****PAYMENT/INVOICES:**

CONTRACTOR shall submit invoices for payment due as provided herein with such documentation as required by Pinellas County and all payments shall be made in accordance with the requirements of Section 218.70 et. seq, Florida Statutes, "The Local Government Prompt Payment Act." Invoices shall be submitted to the address below unless instructed otherwise on the purchase order, or if no purchase order, by the ordering department:

Finance Division Accounts Payable  
Pinellas County Board of County Commissioners  
P. O. Box 2438  
Clearwater, FL 33757

Each invoice shall include, at a minimum, the Contractor's name, contact information and the standard purchase order number. In order to expedite payment, it is recommended the Contractor also include the information shown in below. The County may dispute any payments invoiced by CONTRACTOR in accordance with the County's Dispute Resolution Process for Invoiced Payments, established in accordance with Section 218.76, Florida Statutes, and any such disputes shall be resolved in accordance with the County's Dispute Resolution Process.

**INVOICE INFORMATION:**

**Contractor Information**            Company name, mailing address, phone number, contact name and email address as provided on the PO

**Remit To**            Billing address to which you are requesting payment be sent

**Invoice Date**       Creation date of the invoice

**Invoice Number**       Company tracking number

**Shipping Address**       Address where goods and/or services were delivered

**Ordering Department**   Name of ordering department, including name and phone number of contact person

**PO Number**       Standard purchase order number

**Ship Date**       Date the goods/services were sent/provided

**Quantity**       Quantity of goods or services billed

**Description**       Description of services or goods delivered

**Unit Price**       Unit price for the quantity of goods/services delivered

**Line Total**       Amount due by line item

**Invoice Total**       Sum of all of the line totals for the invoice

Pinellas County offers a credit card payment process (ePayables) through Bank of America. Pinellas County does not charge vendors to participate in the program; however, there may be a charge by the company that processes your credit card transactions. For more information please visit Pinellas County purchasing website at ([www.pinellascounty.org/purchase](http://www.pinellascounty.org/purchase)).

**AGREEMENT****EXHIBIT E - DISPUTE RESOLUTION FOR PINELLAS COUNTY BOARD OF COUNTY COMMISSIONERS IN MATTERS OF INVOICE PAYMENTS:**

Payment of invoices for work performed for Pinellas County Board of County Commissioners (County) is made, by standard, in arrears in accordance with Section 218.70, et. seq., Florida Statutes, the Local Government Prompt Payment Act.

If a dispute should arise as a result of non-payment of a payment request or invoice the following Dispute Resolution process shall apply:

- A. Pinellas County shall notify a vendor in writing within 10 days after receipt of an improper invoice, that the invoice is improper. The notice should indicate what steps the vendor should undertake to correct the invoice and resubmit a proper invoice to the County. The steps taken by the vendor shall be that of initially contacting the requesting department to validate their invoice and receive a sign off from that entity that would indicate that the invoice in question is in keeping with the terms and conditions of the agreement. Once sign off is obtained, the vendor should then resubmit the invoice as a "Corrected Invoice" to the requesting department which will initiate the payment timeline.
  1. Requesting department for this purpose is defined as the County department for whom the work is performed.
  2. Proper invoice for this purpose is defined as an invoice submitted for work performed that meets prior agreed upon terms or conditions to the satisfaction of Pinellas County.
- B. Should a dispute result between the vendor and the County about payment of a payment request or an invoice then the vendor should submit their dissatisfaction in writing to the Requesting Department. Each Requesting Department shall assign a representative who shall act as a "Dispute Manager" to resolve the issue at departmental level.
- C. The Dispute Manager shall first initiate procedures to investigate the dispute and document the steps taken to resolve the issue in accordance with section 218.76 Florida Statutes. Such procedures shall be commenced no later than 45 days after the date on which the payment request or invoice was received by Pinellas County, and shall not extend beyond 60 days after the date on which the payment request or invoice was received by Pinellas County.
- D. The Dispute Manager should investigate and ascertain that the work, for which the payment request or invoice has been submitted, was performed to Pinellas County's satisfaction and duly accepted by the Proper Authority. Proper Authority for this purpose is defined as the Pinellas County representative who is designated as the approving authority for the work performed in the contractual document. The Dispute Manager shall perform the required investigation and arrive at a solution before or at the 60 days timeframe for resolution of the dispute, per section 218.76, Florida Statutes. The County Administrator or his or her designee shall be the final arbiter in resolving the issue before it becomes a legal matter. The County Administrator or his or her designee will issue their decision in writing.
- E. Pinellas County Dispute Resolution Procedures shall not be subject to Chapter 120 of the Florida Statutes. The procedures shall also, per section 218.76, Florida Statutes, not be intended as an administrative proceeding which would prohibit a court from ruling again on any action resulting from the dispute.
- F. Should the dispute be resolved in the County's favor interest charges begin to accrue 15 days after the final decision made by the County. Should the dispute be resolved in the vendor's favor the County shall pay interest as of the original date the payment was due.
- G. For any legal action to recover any fees due because of the application of sections 218.70 et. seq., Florida Statutes, an award shall be made to cover court costs and reasonable attorney fees, including those fees incurred as a result of an appeal, to the prevailing party. If it is found that the non-prevailing party held back any payment that was the reason for the dispute without having any reasonable lawful basis or fact to dispute the prevailing party's claim to those amounts.

AGREEMENT
-----------

**EXHIBIT F - PINELLAS COUNTY INFORMATION SECURITY POLICY****PINELLAS COUNTY INFORMATION SECURITY POLICY**

This policy is  
Authorized by the Pinellas County BTS Board  
and  
Maintained by the Pinellas County Security  
Panel

*Revised and Adopted: August 20, 2021*

**Security Panel Membership as of July 2021:**

Business Technology Services  
Board of County Commissioners  
Clerk of the Circuit Court  
  
Court Administrator  
Property Appraiser  
Public Defender  
Sheriff  
  
State Attorney's Office  
Supervisor of Elections  
Tax Collector

<b>AGREEMENT</b>
------------------

## Table of Contents

<b>I. INTRODUCTION.....</b>	<b>1</b>
A. PURPOSE.....	1
B. APPROACH.....	1
C. EXCEPTIONS.....	1
D. AUTHORITY FOR ACTION.....	1
<b>II. USERS.....</b>	<b>2</b>
A. SUMMARY.....	2
B. SCOPE AND APPLICABILITY.....	2
C. PASSWORDS AND MULTI-FACTOR AUTHENTICATION.....	2
D. PRIVILEGE CONTROL.....	4
E. LOCKING WORKSTATIONS.....	4
F. SOFTWARE.....	5
G. HARDWARE.....	5
H. REPORTING OF SECURITY BREACHES.....	5
I. THIRD-PARTY ACCESS.....	6
J. EMPLOYEE SECURITY AWARENESS TRAINING.....	6
<b>III. APPLICATIONS.....</b>	<b>7</b>
A. PURCHASED OUT OF BOX (“OFF THE SHELF”) APPLICATIONS.....	7
B. APPLICATION DEVELOPMENT.....	7
C. DATABASES.....	9
<b>IV. INFORMATION.....</b>	<b>10</b>
A. SECURITY OF INFORMATION GENERALLY.....	10
B. SCOPE AND APPLICABILITY.....	10
C. PUBLIC RECORDS.....	10
D. ROLES.....	10
E. DATA CRITICALITY.....	12
F. PROTECTED HEALTHCARE INFORMATION.....	13
<b>V. SERVERS.....</b>	<b>14</b>
A. GENERALLY.....	14
B. WEB SERVERS.....	16
C. EMAIL.....	16
D. ORACLE DATABASE SERVERS.....	16
<b>VI. NETWORK SECURITY.....</b>	<b>17</b>
A. ADMINISTRATION.....	17
B. CONNECTIONS.....	17
C. CISCO ROUTERS AND SWITCHES.....	18
D. FIREWALLS.....	18
E. REMOTE ACCESS.....	20
<b>THE IT INFORMATION SECURITY SECTION MUST APPROVE ALL USE OF WIRELESS TECHNOLOGY.....</b>	<b>20</b>
<b>VII. VULNERABILITY ASSESSMENTS AND NETWORK SCANNING.....</b>	<b>22</b>
A. GENERALLY.....	22
B. ASSESSMENTS BY THE IT DEPARTMENT.....	22
C. ASSESSMENTS BY AGENCIES.....	22
D. ASSESSMENTS BY THIRD PARTIES.....	22
E. LEGAL REQUIREMENTS.....	22
<b>VIII. COMPUTER INCIDENT RESPONSE TEAM (CIRT).....</b>	<b>23</b>
<b>IX. VOLUNTEERING OF INFORMATION TECHNOLOGY SERVICES WITHIN PINELLAS</b>	

**AGREEMENT****I. Introduction****A. Purpose**

The purpose of this Information Security Policy is to:

- Protect information technology
- Minimize liability and determine acceptable risk related to information and information technology
- Assign responsibility and roles for information and information technology

The intent of this Information Security Policy is not to restrict or inhibit an Agency's ability to perform business activities through the use of information or information technology.

**B. Approach**

The approach taken in writing this Security Policy is based on the "weakest link" principle. In other words, since all components of information technology are interrelated (a chain), the overall strength of information security is determined by the weakest security employed on a component of information technology. Information security can no longer be a concern of technical specialists alone--it must instead be addressed by everyone.

**C. Exceptions**

Any exceptions to the Information Security Policy will be approved by the respective Appointing Authority and the Department of Information Technology Security Section. If a conflict exists, the matter will be reviewed by the Pinellas County Information Security Panel and presented to the Information Technology Board.

**D. Authority for Action**

The IT Information Security Officer shall have the authority to take action consistent with this Policy to protect the Enterprise network and associated systems.

**AGREEMENT****II. Users****A. Summary**

Users conduct a great deal of business by the use of computer devices and networks. To this end, this Policy provides information security instructions applicable to all users (employees and third parties) who use computer systems. All users are expected to comply with this Policy as a condition of continued employment or access to the Enterprise Network.

**B. Scope and Applicability**

This Policy applies to the handling of all production information, regardless of the origin of this information (card holder transactions, third party market research, etc.). "Production information" is information routinely used to perform business activities. This Policy applies regardless of the information technology used, regardless how the information is employed to meet business needs, and regardless which users have access to the information and information technology. This Policy applies to all Pinellas County agencies, all other agencies that use Pinellas County information and Pinellas County information technology, and all third-parties who have access to Pinellas County information and information technology. This Policy applies to any electronic device that connects to the Pinellas County network or contains Pinellas County data.

**C. Passwords and Multi-Factor Authentication****1. Minimum Password / Passphrase Length**

All system administrators must define a minimum password/passphrase length commensurate with the level of security required. For all systems, a minimum length of fourteen (14) characters is to be used when feasible, otherwise use the maximum that the system allows. When a system has the capability of automatically enforcing a minimum length, this ability shall be activated.

**2. Multi-Factor Authentication**

Where possible, multi-factor authentication will be employed for all user accounts.

**3. Complex Passwords / Passphrases**

Password complexity is not mandated unless explicitly demanded for an Appointing Authority due to compliance requirements such as the BTS CJIS Security Policy. System Administrators should compare prospective passwords/passphrases against the list of known bad passwords/passphrases, when possible. Users must use difficult to guess passwords/passphrases on systems that do not automatically generate appropriate passwords/passphrases. A difficult-to-guess password is one which does not consist of one type of character, and which does not appear in any dictionary. For example, a password with all letters or all numbers would not be appropriate. Common character sequences such as "123456"



**AGREEMENT**

also must not be employed. Personal details such as a spouse's name, license plate number, social security number, and birthday must not be used unless accompanied by additional unrelated characters.

**4. Cyclical Passwords / Passphrases Prohibited**

Users are prohibited from constructing fixed passwords/passphrases by combining a set of characters that do not change, with a set of characters that predictably change. In these prohibited passwords, characters which change are typically based on the month, a department, a project, or some other easily guessed factor. For example, users must not employ passwords/passphrases like "JAN2021" in January, "FEB2021" in February, or "Summer2020" and "Fall2021".

**5. Password / Passphrase Reuse Prohibited**

Users may not reuse a password/passphrase unless at least twelve (12) months has passed since the password/passphrase was last used. Systems with the capability to enforce this automatically should have this ability turned on.

**6. Storage of Passwords / Passphrases**

Users must maintain exclusive control of their personal passwords; they must not share them with others. Passwords/passphrases must not be stored in readable form in files, browsers, terminal function keys, in computers without access controls or in other locations where unauthorized persons might discover them. This includes unsecured paper or other written records. Where systems and applications that support managed service accounts, password/passphrase managed service applications should be used when possible for service account and password/passphrase login maintenance.

**7. Expiration of Passwords / Passphrases**

Passwords/passphrases are required to be changed every ninety (90) days unless MFA is initiated, then timeframe may be extended to 180-days.

**8. Timeout / Lockout**

Where possible, users shall have a maximum of six (6) attempts to enter the correct password. Failure to do so may result in a lockout period not to be less than thirty (30) minutes.

**9. System Access control with Individual Passwords / Passphrases**

Information technology access control to production Enterprise systems must be achieved via passwords/passphrases that are unique to each individual user, excluding systems intended for public viewing applications.

**10. Changing of Vendor-Supplied Default Passwords Passphrases**

Whenever any computer system or device has a vendor-supplied default password/passphrase enabled, this password/passphrase must be disabled or changed prior to the system or device being placed in service.

**AGREEMENT****D. Privilege Control****1. Permissible Uses of Information**

Information and information systems must be used only for the business purposes expressly authorized by management.

**2. Existence of User Access Capabilities Does Not Imply Permission**

Users must not read, modify, delete, or copy a file belonging to another user without first obtaining permission from the owner of the file or someone else authorized to grant such permission. Unless general user access is clearly provided, the ability to read, modify, delete, or copy a file belonging to another user does not imply permission to actually perform these activities.

**3. Reporting Changes in User Duties to Systems Administrators**

Management must promptly report all significant changes in end-user duties or employment status to the computer system administrators handling the user-IDs of the affected persons.

**4. All System Access Privileges Cease When Access is No Longer Required**

All information systems privileges must be promptly terminated at the time that a user ceases to provide services that require access.

**5. Browsing is Prohibited**

Users must not browse through computer systems or networks. For example, curious searching for interesting files and or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job are not considered browsing.

**6. External Connections Require Approval**

Access to Pinellas County internal networks from remote locations including homes, hotel rooms, and customer offices, must in all instances be approved in advance by the involved user's immediate manager. In addition, the IT Information Security Section must be notified prior to the implementation of such access.

**E. Locking Workstations**

Employee workstations should be locked, and password protected when not in use by users. This can be accomplished by manually locking the workstation before leaving or preferably by utilizing an automated locking method with a reasonable timeframe for auto locking.

**AGREEMENT****F. Software****1. Application Software**

Users should not install any software programs on computers without obtaining advance permission from management.

**2. Operating System Software**

Users must not change operating system configurations, upgrade existing operating systems, or install new operating systems on any devices without obtaining advance permission from their Agency management.

**3. Virus Program Installed**

All systems must run virus detection software that has been approved by the IT Information Security Section if such software is commercially available. The software must run each time the machine is turned on and whenever external storage media is supplied (floppy and zip disks).

**a) Current Pattern Files**

All virus protection programs must utilize current scanning files (pattern files) when made available by the virus protection software vendor.

**b) Internet Software Must be Scanned for Viruses Prior to Execution**

Any software, which is received as an E-mail attachment or by any other resources of the Internet, must be written to a secondary storage device such as a hard drive prior to executing the software. This is to ensure that the software is scanned by the users' virus protection software.

**c) Virus Programs May Not be Disabled**

Users may not disable virus detection programs.

**4. Management Review of End-User Backup Process**

Department managers or their delegates must make sure that proper backups of sensitive, critical and valuable data are being made if such data is resident on microcomputers (PC), workstations, or other small systems.

**G. Hardware**

Users should not install any hardware on personal computers without obtaining advance permission from management.

**H. Reporting of Security Breaches**

Any issues related to security breaches such as viruses and unauthorized access should be reported to the users' systems administrator. The systems administrator shall report security-related incidents to the IT Information Security Officer.

**AGREEMENT****I. Third-Party Access****1. Contractors and Contracted Individuals**

Before such third parties are given access to systems, a contract defining the terms and conditions of such access must have been signed by a responsible manager or principal of the third party organization. The contract must include a statement that the third party will abide by this Security Policy.

**2. Non-Contracted Third Parties**

Such third parties must only be granted access to computers or networks with agency approval.

**3. Third Parties Must Agree Not To Disclose Sensitive Security Information**

Third Parties must agree in writing prior to beginning work not to reveal sensitive security information to non-employees without permission from the hiring Agency.

**4. Third Parties and Their Own Computers**

Third parties must not connect their own electronic devices or personal computers to the Enterprise network unless they have received prior approval by Agency management.

**J. Employee Security Awareness Training**

Every entity shall establish and maintain a formal security awareness program to make all personnel aware of the importance of information security.

- The program shall provide multiple methods of communicating awareness and educating personnel.
- Personnel must complete security awareness training during new employee orientation and at least annually thereafter.
- BTS shall provide a compliant solution to facilitate security awareness training for all entities.
- Appointing Authorities may authorize employee access accounts be disabled if security awareness training is not completed in accordance with this policy.
- Personnel that do not complete training in compliance with this policy may be subject to disciplinary action.
- Personnel may incur loss of financial or personal data that could have impact to the employees outside the scope of their employment if they disclose their username and password to an unknown third party or malicious actor.

**AGREEMENT****III. Applications****A. Purchased Out of Box ("Off the Shelf") Applications**

Agencies are responsible for the security of out of the box applications.

**B. Application Development****1. Generally****a) Applications Developed with Security in Mind**

Before a new application is developed, Agency management must have clearly specified the relevant security requirements.

**b) Design Conforms to Established Standards**

Agency management must ensure that all software development and software maintenance activities performed by in-house staff or third parties subscribe to Pinellas County policies, standards and procedures as they relate to security.

**c) Development Tasks Performed by Appropriate Personnel**

Software development will be performed by staff or third parties tasked with that responsibility, with exceptions as approved by Agency management.

**2. Development by Third Parties****a) Subject to Same Security Policies as In-House Development**

All third party development is subject to Section III. B, 1 of this Policy.

**b) Source Code Remains with the Agency Upon Departure**

Source code developed by outside personnel under contract shall remain with the Agency in the same manner as software developed internally upon the departure of the third party. The contracting Agency and/or the Department of Information Technology shall make arrangements for the safe storage and retention of such source code.

**c) Developed Applications for Critical Production Use**

If a third party developed application is being considered, and if this software will be used for a critical business activity, one of two conditions must be met prior to completing the transaction. The first condition is that the third party must license any developed intellectual property to the Agency. The second condition is that the third party must periodically provide any developed intellectual property to a mutually agreed on party who will hold it in escrow. This Policy allows the Agency staff to continue to maintain the software even though the third party may have gone out of

**AGREEMENT**

business, may have discontinued the product, or may be negligent in terms of fixing problems in the code.

d) Passwords and User Accounts

When it is necessary for third parties to be given access to systems, special accounts with the permissions necessary for the job shall be set up for their exclusive use. Such accounts will be deleted or disabled upon the termination of the third party's employment. Passwords for accounts used by IT staff or employees shall not be given to third parties. If this is not possible, any passwords a third party may have been given or been exposed to shall be changed upon the termination of the third party's employment.

3. Application Security

a) No Undocumented Access Methods

Programmers and other technically-oriented staff must not install back doors that circumvent the authorized access control mechanisms found in operating systems and/or access control packages.

b) Test Data Clearly Identified and Separated From Production

Software in development and its data must be kept strictly separate from production software and its data. If facilities permit it, this separation must be achieved in physically separate computer systems. When computing facilities do not allow this, separate directories or libraries with strictly enforced access controls must be employed.

4. Application Development

a) Development Methods

Because unfamiliar programming languages can pose a security risk, the introduction of tools and languages not previously used in production work shall be reviewed and must be approved by Agency management. For third-party development, the contracting Agency must grant approval for new tools and languages.

b) Developer Access Privileges Limited

Application development staff must not be permitted to access production information, with the exception of the production information relevant to the particular application on which they are currently working.

5. Application Testing

a) Access to Production Data Restricted

Where access to production information is required so that new or modified applications may be developed or tested, only "read" and "copy" access may



<b>AGREEMENT</b>
------------------

be granted to production systems. This access is permitted only for the duration of the project and must be promptly revoked upon its completion.

b) Special Certification Required

In rare circumstances an in-house or third party development project can have a direct impact on human safety. In such instances, management must certify to the IT Board that necessary security controls are in place, functioning, and have been thoroughly tested.

6. Mission Critical Applications

All software that handles sensitive or critical information, and that has been developed in-house or by third parties, must have its security controls fully operational prior to being placed in production.

**C. Databases**

1. Applicability

This section of the Security Policy applies to all production databases.

2. Database Updates Must be Made Only Through Established Channels

Updates to production databases must only be made through established channels that have been approved by Agency management. Unless authorized by Agency management, the use of direct database access utilities in the production environment is not permitted.

**AGREEMENT****IV. Information****A. Security of Information Generally**

Information is no longer something which supports the provision of a product or service. Information itself has become the product or service that many entities provide. The new centrality of information necessitates the establishment of new roles and responsibilities to properly manage and protect it. To this end, this Policy defines the information security roles and responsibilities of Owners, Managers, and Users.

**B. Scope and Applicability**

This section applies to the handling of all production information, regardless of the origin of this information. "Production information" is information routinely used to perform important business activities or routinely used to support management decision-making. This Policy applies regardless of which information handling technology is used, where the information resides, how the information is employed to meet business needs, and which users have access to the information. This applies to all Pinellas County agencies, all other agencies which use Pinellas County networks, and third parties who have access to production information.

**C. Public Records**

Ch.119, Fla. Stat. (2000) provides that most records produced in the course of government business are public and are open to inspection by anyone who asks. The law further provides that the Information Owner (generally elected officials) may reasonably regulate the time and manner of such inspections. The law also assigns responsibility for the security of information. The fact that a particular piece of information is public record does not mean that it may be disclosed in any manner that an employee or contractor may see fit, nor does it excuse security breaches or other violations of the security Policy by anyone.

**1. Access to Information**

All information is to be accessed in the manner approved by the Owner responsible for it, using systems and access methods designed by technology staff for that purpose.

**2. Exemptions From Public Records Law**

Certain information is exempt from Ch. 119, Fla. Stat. (2000). Among the categories is security information. System passwords, user accounts, and other information directly related to security are not open to public inspection.

**D. Roles****1. Information Owners (Elected and Appointed Officials and their designees)**

The term "owner" to government must necessarily have a different meaning than in the private sector. An Information Owner in a government context means that

**AGREEMENT**

person or persons who are legally charged with and granted the authority for acquiring, creating, and maintaining information and information systems within their assigned area of control.

a) Responsibilities of Information Owners

- Categorizing the criticality of information for which they have been designated as Owner.
- Authorizing User access to information.
- Deciding permissible uses of information.
- Approving relevant controls for information consistent with policies and standards.
- Understand the uses and risks associated with the information for which they are accountable, including their responsibility for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security related control deficiencies.
- Provide Users with sufficient time to receive periodic information security training.

b) Information Ownership Assignment

The Information Owner must specify the assignment of information ownership responsibilities for databases, master files, and other shared collections of information. The Information Owner is also responsible for designating the individuals who will maintain access rights to these information collections on behalf of the owners.

c) Authority for Information Owners

The authority for Information Owners (generally elected or appointed officials or their designees) is set forth in Ch. 119, Fla. Stat. (2000), the Florida Constitution, and other laws.

2. Information Managers

Information Managers are individuals (Agency IT personnel, systems administrators or Department of Information Technology staff) who have been granted physical or logical possession of information by Owners.

a) Responsibilities of Information Managers

- Provision, monitoring, and maintaining of information systems services consistent with the instructions of Owners and consistent with the policies and standards issued by the Information Technology Board.
- Protecting the information in their possession from unauthorized access, alteration, destruction, or usage.
- Providing and administering general controls such as backup, recovery, and updates of virus protection files.

**AGREEMENT**

## b) Production Changes Prohibited

Information Managers are forbidden from changing the production information in their possession unless they have received explicit permission from either the Owner or an authorized User.

## c) System Administrators

System administrators are individuals that are empowered or tasked with the administration of computer systems.

(1) System administrators should follow the best practices documents for the environments that they maintain.

(2) To further ensure compliance, agencies should incorporate policy and best practice compliance as part of the performance evaluations for employees that administer systems.

## 3. Information Users

Information Users are individuals who have been granted explicit authorization to access, modify, delete, and/or utilize information by the Owner.

## a) Responsibilities of users

- Use information only for the purposes specifically approved by the Owner.
- Comply with all security measures defined by the Owner, implemented by the Manager, and/or defined by this Policy or other Agency policies.
- Refrain from disclosing information in their possession without first obtaining permission from the Owner.
- Report to the Information Manager all situations where they believe an information security vulnerability or violation may exist.

## b) Special Responsibilities

Users may have special responsibilities, such as backup and virus screening, which are defined in the User section of this Information Security Policy.

**E. Data Criticality**

## 1. Web and Commerce Servers Must Not Store Critical Information

Web and commerce servers must not be used to store any critical information such as credit card numbers, credit references, and social security numbers.

**AGREEMENT****2. Labels for Collections of Information with Various Sensitivities**

When information of various sensitivity classifications is combined, the resulting collection of information must be classified at the most restricted level found anywhere in the sources.

**3. Erasure of Sensitive Information**

Sensitive information must be made unrecoverable on the storage media prior to disposal or transfer of the assets.

**4. Regular Purging of Information Which Is No Longer Needed**

All information must be destroyed or disposed of when no longer needed pursuant to applicable records retention guidelines. To support this Policy, management must review the continued value and usefulness of information on a periodic and scheduled basis.

**5. Electronic Media Disposal**

To ensure the proper and secure handling of sensitive electronic information or data, all storage systems or devices will follow the "Best Practices document for Electronic Media Disposal".

**F. Protected Healthcare Information****1. Health Information Portability and Accountability Act**

Agencies or departments that are designated as "Covered Entities" that deal with Protected Health Information (PHI) data, must ensure they are compliant with the most recent HIPAA/HITECH regulations. Covered Entities should work with their designated HIPAA compliance officer to ensure compliance.

**AGREEMENT****V. Servers****A. Generally****1. Environmental Concerns****a) Climate Control for All Servers**

All servers must be located in climate control areas where the temperature and humidity can be adjusted to meet the hardware requirements.

**b) Power/UPS considerations**

All servers must have uninterruptible power systems (UPSs).

**2. Physical Security****a) Location**

Areas that house servers must be protected with physical security measures that prevent unauthorized persons from gaining access.

**b) Moving Servers Without Approval Prohibited**

Servers must not be moved or relocated without the prior approval of the involved department manager.

**3. Communications****a) Servers Protected by the County Firewall**

All servers must be protected by the County firewall or by a firewall approved by the IT Information Security Section.

**b) Approval Required For Systems Accepting In-Coming Dial-Up Calls**

Connections must not be made to any servers that accept in-coming-dial-up calls unless the IT Information Security Section has first approved them. Servers must comply with the remote access section of this Policy.

**c) Internal Servers Shall Not Be Directly Accessed from the Internet.**

Internet access to internal servers shall take place only through a web server or some other intermediate computer that is dedicated to Internet activity.

**4. Best Practices**

All servers should conform to security best practices as supplied by the IT Information Security Section and approved by the Information Security Panel.



<b>AGREEMENT</b>
------------------

**5. Backup and Retention**

Although backup procedures may vary from system to system, the following general procedures should apply to all production systems.

a) Data Must be Archived to follow Pinellas County Government Records Management Division's Guidelines

All data must be archived following the guidelines of Pinellas County Government Records Management Division or the State of Florida General Records Schedule GS1 – State and Local Government Records Manual.

b) Verification required

Verification of the proper operation of the backup equipment and media shall be performed on a regular basis. If time and equipment permit, such verification should be performed when backups are made.

c) Off-Site Storage of Backup Media

Backups of essential business information and software must be stored in an environmentally protected and access-controlled site that is a sufficient distance away from the originating facility to escape a local disaster.

**6. Virus Program Installed**

All servers must run virus detection software that has been approved by the Information Security Section. This software must have current pattern files, must run each time the machine is turned on, and whenever removable storage media is introduced. In the event that the software industry does not provide virus checking for a particular server platform, some form of file integrity checking will be implemented for that particular server platform.

**7. Logging**

All unauthorized access to servers must be logged using best practices. The logging is subject to the same policies regarding "Backup and Retention".

**8. Administration of User Access Rights**

Access rights are given to users only to the extent that they need to fulfill their job responsibilities.

**9. Locking Servers**

Servers should be locked and password protected when not in use by system administrators. This can be accomplished by manually locking the server before leaving or preferably by utilizing an automated locking method with a reasonable timeframe for auto locking.

**AGREEMENT****B. Web Servers****1. Must Adhere to Server Security Policies**

All web servers, which are intended for access by the public (Internet Community), must adhere to the same security policies related to servers. In addition to the related server policies, web servers should adhere to the Best Practices for Web Servers document.

**2. Specific Procedures Required for Internet Web Servers**

All Internet-connected web servers must be "hardened" according to industry standards and manufacturer's recommendations. Additionally, the IT Information Security Section shall conduct a scan for known vulnerabilities before a server is connected to the Internet. All known vulnerabilities must be corrected prior to the server being placed in production.

**C. Email****1. Message and Attachment Security**

All incoming emails must be scanned by antivirus software updated with current signatures. Messages and/or attachments found to pose a threat will be quarantined or deleted, and the system administrator will take appropriate action.

**2. Automatic Deletion**

Because certain types of email attachments are known to carry a high risk of malicious code, the IT Department may delete such attachments preemptively.

**3. Unsolicited Email**

The sending of unsolicited commercial email ("Spam") is prohibited. Email servers shall be configured to disallow "relaying" of messages that do not originate on the County network. This Policy shall not be construed to prohibit "opt-in" mailing lists, or other legitimate business uses of email.

**4. Message Confidentiality**

Emails are sent in plain text and pass through multiple servers and devices, which may present opportunities for loss of privacy. When sending sensitive data via Email over the Internet, encrypting the message is required to maintain the confidentiality of the data. Unencrypted email is not a secure method for transmitting sensitive information such as Protected Healthcare Information (PHI), Personally Identifiable Information (PII) or Credit Card information.

**D. Oracle Database Servers**

All Oracle database servers should follow the Oracle Best Practices document as well as the appropriate server best practices documents.

**AGREEMENT****VI. Network Security****A. Administration****1. Time-Out After No Activity**

Systems accepting remote connections from public networks such as the dial-up phone network or the Internet must be configured to terminate all sessions after one (1) hour of inactivity.

**2. Internal Network Addresses Must Not Be Disclosed**

The internal system addresses, configurations, and related system design information for networked computer systems must be restricted such that both systems and users outside Pinellas County's internal network cannot readily access this information.

**3. E-Government Web Servers Must Be In Demilitarized Zone (DMZ)**

All E-Government web servers must be protected by firewalls in a demilitarized zone.

**4. Inventory of Connections To External Networks**

The IT Information Security Section must maintain a current inventory of all connections to external networks including, EDI networks, extranets, and the Internet.

**B. Connections****1. Changes to the Enterprise Network**

Changes to Enterprise networks must only be made by authorized members of the IT Department and approved by the Telecommunications Operations Section, in conjunction with the IT Information Security Section.

**2. Installation of Communications Lines**

Users and vendors must not make arrangements for, or actually complete the installation of data lines with any carrier, if they have not first obtained approval from the manager of the Telecommunications Operations Section, in conjunction with the IT Information Security Section.

**3. Physical Security of Communications Equipment**

Buildings which house communications equipment must be protected with physical security measures that prevent unauthorized persons from gaining access.

**4. Subscription to External Networks**

Users must not establish connections with Internet Service Providers (ISPs) or other external networks while connected to the Enterprise Network unless this arrangement has first been approved by the IT Information Security Section.

**AGREEMENT****5. Modems Connected to Devices on the Enterprise Network**

Agency management and the IT Information Security Section must approve all modems connected to the Enterprise network.

**C. Cisco Routers and Switches**

All Cisco routers / switches should conform to the Best Practices document for Cisco Devices.

**D. Firewalls****1. Firewall Applicability****a) Connections that Require Approved Firewalls**

All connections between Pinellas County internal networks and other networks or computers approved by the IT Information Security Section must include an approved firewall.

**2. Administration****a) Firewall Configuration Changes Require Approval**

Perimeter commercial firewall configuration changes require IT Information Security Section approval.

**b) Defined Decision Maker**

Before being enabled, all new firewall services and new connectivity paths must be evaluated in terms of security risks. The IT Information Security Section is the recognized decision maker who can either approve or deny these requests.

**c) Default To Denial**

Every external connectivity path and Internet service not specifically permitted by a firewall rule must be blocked.

**d) Security Diagrams**

Prior to the deployment of any firewall, a diagram of permissible paths with a justification for each must be submitted to the IT Information Security Section. Permission to enable any paths must be approved by the IT Information Security Section.

**e) Logs**

**AGREEMENT**

All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. In addition, all suspicious activity that might be an indication of unauthorized usage or an attempt to compromise security measures must also be logged. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

f) Contingency Planning

Technical staff working on firewalls must prepare and obtain IT Information Security Section approval for contingency plans which address the actions to be taken in the event of various problems including system compromise, system malfunction, and power outage. These contingency plans must be kept up-to-date and tested.

g) Firewall Access Privileges

Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few individuals. These privileges must be granted only to individuals who are employees of respective agencies (no temporaries, contractors, consultants, third parties, or outsourcing personnel). At least two staff members must be adequately trained in firewall administration.

h) Back-Up

Current off-line back-up copies of the firewall configuration must be maintained at all times and be immediately available.

i) Firewall Dedicated Functionality

Firewalls must run on dedicated machines that perform no other services. To reduce the chances of security compromise, firewalls must have the bare minimum of software resident on them.

j) Posting Updates

Unless approved in advance by the IT Information Security Section, staff members responsible for administering firewalls must install and run these updates as appropriate.

k) Firewall Physical Security

All firewalls must be situated in restricted areas.

l) Firewall Failure

In the event of firewall failure remote connectivity must not be allowed.

<b>AGREEMENT</b>
------------------

## m) Firewall Best Practices

Those that administer network firewalls will adhere to the Pinellas County Network Firewall Best Practices document.

## 3. Intrusion Detection

All firewalls must include intrusion detection systems approved and configured to the specifications defined by the IT Information Security Section.

## 4. Monitoring Vulnerabilities

Staff members responsible for administering firewalls must use relevant resources that provide current information about security vulnerabilities. Any vulnerability that appears to affect the enterprise networks, systems, or applications must promptly be brought to the attention of the IT Information Security Section.

**E. Remote Access**

## 1. Use of Broadband for Business Communications

To access the enterprise network, Internet connections must have an approved firewall installed, virus protection and a virtual private network (VPN).

## 2. Strong Authentication Required For Dial-Up

To positively identify the calling party, all dial-up connections to the enterprise network must employ strong authentication.

## 3. Inbound Dial-Up to Networks

All inbound dial-up lines connected to the enterprise networks must pass through a RAS/modem pool and an approved firewall.

## 4. Using Wireless Technology for Data

The IT Information Security Section must approve all use of wireless technology.

## 5. Wireless LAN (802.11, WLAN)

All wireless LANs must follow Pinellas County's "Wireless LAN (802.11, WLAN) Best Practices".

## 6. Clientless VPN



**AGREEMENT**

All implementations of clientless VPN will follow Pinellas County's "Clientless VPN Best Practices" or be approved by the IT Information Security Section.

7. Request and Approval of VPN Access

All requests for Enterprise VPN access must be submitted to the IT Customer Support Center via the approved form. Agencies, based on justification and legitimate business purposes, will be responsible for the approval of VPN access.

**AGREEMENT****VII. Vulnerability Assessments and Network Scanning****A. Generally**

All County systems and IT-related procedures shall be subject to periodic vulnerability assessments at the policy, procedural, application, system, and network levels. The IT Security Management Section, with the approval of the IT Information Security Panel, shall determine the frequency and type of enterprise assessments. However, with the approval of agency management, agency-specific assessments can be performed by the IT Security Management Section as long as the Security Panel membership is notified.

**B. Assessments by the IT Department**

Assessments conducted by the IT Department shall be coordinated with agency management and IT staff. Efforts shall be made to minimize adverse effects of such assessments.

**C. Assessments by Agencies**

Because vulnerability scanning can adversely affect network services for the entire enterprise, no agency shall conduct or contract for a vulnerability assessment without coordinating these efforts with the IT Information Security Section. The IT Information Security Section shall notify the appropriate areas of the IT Department as necessary, as well as agencies which may be affected by the assessment activities.

**D. Assessments by Third Parties**

All assessments conducted by third parties shall be done in conjunction with the IT Information Security Section. The terms of the engagement must be acceptable to the contracting agency and the IT Information Security Section. The assessment shall be conducted so as to minimize the possibility of disruption to other agencies.

**E. Legal Requirements****1. Required Assessments**

Some assessments are required to be conducted by law or by contract. This policy shall be followed in those situations unless specifically provided otherwise by law. The IT Information Security Section shall be notified of any such assessment.

**2. Confidentiality of Assessment Results**

Results of vulnerability assessments shall not be published or made available as public records to the extent provided by Florida law. Third party service providers shall be required by contract to maintain confidentiality. Agency and IT personnel shall only share and discuss the results with personnel authorized by their appropriate management.

**AGREEMENT****VIII. Computer Incident Response Team (CIRT)**

Computer-related incidents will be addressed according to the Pinellas County CIRT Manual.

**IX. Volunteering of IT Services within Pinellas County Government****1. Introduction**

Pinellas County Government is frequently approached by individuals, groups, or organizations offering to volunteer their services at no cost to the County. While this may be of mutual benefit in many operational areas of the government, such practice within Information Technology imposes significant security risks of the applications, workstations, systems, networks, and information that must be protected. Given this, the following policies shall be followed in order to maintain an acceptable level of risk in our work practices.

**2. Volunteering of Information Technology services that involve setup or maintenance of infrastructure including but not limited to servers, networks, databases, applications, and workstations**

Work related to setup or maintenance of IT infrastructure requires access rights that are only granted to qualified and trained personnel. Such personnel may include paid employees or contractors, both of whom have responsibility and accountability for the work they perform. Authorization for such access shall not be provided to any volunteer worker operating in this capacity.

**3. Volunteering of Information Technology administrative services including but not limited to data entry, routine office tasks, and poll workers**

The use of volunteers for office tasks, such as routine data entry, office work, poll workers, etc. is subject to agency policies and procedures. Agencies should have a policy in place regarding access to facilities and information, and closely supervise volunteers who work with potentially sensitive data or in areas containing equipment with access to sensitive data. Volunteers should be restricted from access to server and network infrastructure, and should be given their own logon credentials for systems they are authorized to access. Such credentials shall be restricted to the work the volunteer is authorized to perform.

**4. Other Volunteer Services**

Nothing in this Policy shall prohibit the use of volunteer focus groups, testing of applications intended for public use, or other frequently used means of involving the public in government activities.

<b>AGREEMENT</b>
------------------

**X. Patch Management**

All servers, workstations, and firewalls should follow the Patch Management Best Practices document. Justification as to non-conformance to this Best Practice will be documented for that agency.

**AGREEMENT****XI. Glossary**

**Access Control** - A System or method designed control access to systems, networks, applications, or data. Access control ensures appropriate access to computer resources.

**Application** - A software program that carries out some useful task. Database managers, spreadsheets, communication packages, graphics programs, and word processors are all applications.

**Backdoor** - A way of breaking into password-protected applications, systems, or networks without using the assigned password. Also, a program that provides unauthorized access to an application, system, or network.

**Broadband** - Typically refers to cable modem or DSL access. Broadband provides faster access than dial-up access.

**Clientless VPN** - A technology that provides remote access connectivity to the organization's protected resources (including but not limited to systems, applications, and networks) from almost any Internet-enabled location. Typically, this is accomplished using a Web browser and the browser's native SSL encryption capabilities.

**Commerce Server** - A computer system, typically an Internet Web Server, through which business and transactions are conducted over the Internet.

**Dial Up** - A connection to the Internet, or any network, where a modem and a standard telephone line is used to make a connection between computers.

**DMZ (Demilitarized Zone)** - A portion of the network where computers are shielded, from both the trusted network and the un-trusted network, by a firewall.

**DSL - Digital Subscriber Line**. A broadband technology that transmits data over a regular phone line. A DSL circuit is much faster than a regular phone line.

**EDI - Electronic Data Interchange** - A set of standards that provide computer-to-computer exchange of data. These standards, for example, allow for transmission of payments, purchase orders, shipping documents, and invoices between computer systems.

**Electronic Devices - (Mobile Devices)** - Wireless devices such as cell phones, personal digital assistants (PDA's), and pagers that can be held in the palm of a user's hand.

**Encryption** - The transformation of data into a form unreadable by anyone. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it was not intended. In security, encryption is the ciphing of data by applying an algorithm to plain text.

**Enterprise Network** - A conduit for which data is transmitted throughout an entire

<b>AGREEMENT</b>
------------------

organization.

**Firewall** – A collection of hardware and software that limits the exposure of protected data, applications, computers and networks from outside the organization.

**Hardened (i.e. Web Servers)** – A set of procedures made to a computer system which makes the computer system resistant to hacking attempts.

**Multi-Factor Authentication** – Also known as “two-factor” authentication. Can be used to authenticate to an application, system, or network. It is a combination of what the authorized users knows (such as a password) and what the users possesses (such as a smart card or soft token).

**Owner (Elected Official/Appointing Authority)** – In government, a person or persons who is legally charged with granting the authority for acquiring, creating, and maintaining information and information systems within their assigned area of control.

**Perimeter Commercial Firewall** – Firewalls that control connections between an organization’s protected enterprise network and other outside networks such as the Internet.

**RAS – (Remote Access Server)** – A combination of computer hardware and software that is connected to an enterprise network and provides authentication and network access services for incoming dial up connections.

**Source Code** – A set of instructions, written in a programming language, that must be translated to machine instructions before the program can run on a computer. It is typically a programmer that creates source code. The program that finally runs on that computer is known as the object code.

**Systems Administrator** – Agency level individuals in charge of multi-user systems. Generally, systems administrators are in charge of programming, support, security, and storage multi-user systems.

**Third Party** – An organization or individual that is not an employee of Pinellas County nor are they an employee of agencies belonging to the enterprise network.

**Users** – Individuals who have been granted explicit authorization to access, modify, delete and/or utilize information by the owner.

**VPN (Virtual Private Network)** – A combination of hardware and software, that uses authentication and encryption to provide a secure method of communicating over public networks, such as the Internet. The encryption scrambles all of the data sent through the public network, by the VPN, so that communications are “virtually” private.

**Wireless Technology** – Transmission of data using radio waves.