

MK15-1020

PROFESSIONAL SERVICES CONTRACT BETWEEN
THE OFFICE OF INSPECTOR GENERAL/CITY OF NEW ORLEANS
AND
ULTIMATE TECHNICAL SOLUTIONS, INC.

THIS AGREEMENT ("Agreement") is entered into this 21 day of Sept, 2015, but shall be effective as of September 30, 2015 ("effective date"), by and between the City of New Orleans/Office of Inspector General, represented by Mitchell J. Landrieu, Mayor, ("City") and Ultimate Technical Solutions, Inc. ("UTSI" or "Contractor"), who hereby agree as follows:

WHEREAS, the Contractor has the requisite expertise, qualifications, and certifications in place and available for the performance of the professional services required under this Agreement;

NOW THEREFORE, the City and the CONTRACTOR, for the consideration and under the conditions set forth, do agree as follows:

I. THE CONTRACTOR'S OBLIGATIONS.

A. Services. The Contractor will:

1. Provide set up and configuration services for new IT hardware and software, and other ancillary services as required.
2. Submit complete and accurate invoices, maintain records, submit to audits and inspections, maintain applicable insurance, and perform all other obligations of the Contractor set forth in this Agreement;
3. Promptly correct any errors or omissions and any work deemed unsatisfactory or unacceptable by the OIG, at no additional compensation;
4. Monitor, supervise, and otherwise control and be solely responsible for all persons performing work on its behalf;

OIG officers and employees are not authorized to request or instruct the Contractor to perform any work beyond the scope or duration of this Agreement in the absence of an executed amendment to this Agreement.

B. Key Personnel

The only Contractor personnel who will perform work pursuant to this Agreement are listed in Attachment I, Fee Proposal and Key Personnel, attached hereto and made a part of this Agreement. Contractor has provided current resumes for all personnel. The Contractor's personnel assigned to this Contract may not be replaced without the written consent of the OIG. Such consent shall not be unreasonably withheld or delayed provided an equally qualified replacement is offered. Contractor must provide a resume demonstrating adequate qualifications, prior to work commencement, of any personnel substitutions. All Contractor personnel who will perform work at the OIG will sign the Information Technology and

Information Systems Rules of Behavior and Confidentiality Agreement, attached hereto as Attachment II, prior to doing any work on OIG computer systems. All Contractor personnel who will perform work at the OIG will undergo a background check.

C. Compliance with Laws. The Contractor, and any person performing work on its behalf, will comply with all applicable federal, state, and local laws and ordinances.

D. Invoices.

1. The Contractor will submit invoices for work performed under this Agreement to the OIG no later than ten (10) calendar days following the completion of work performed. Untimely invoices may result in delayed payment for which the City/OIG is not liable. At a minimum, each invoice must include the following information:

- a. Description of the work completed and the individuals who performed the work;
- b. An authorized signature under penalty of perjury attesting to the validity and accuracy of the invoice.

2. Invoices will be processed upon OIG's written acknowledgement of receipt of the satisfactory work products.

3. The OIG has the sole right to approve or require changes to the form of the invoice. The OIG may require additional supporting documentation to be submitted with invoices.

4. The OIG retains the right to cancel this contract at any time if it determines that the work being provided by the contractor is not of adequate quality or the contractor is non-responsive to requests for services.

E. Records and Reporting.

1. The Contractor will maintain all documents (in any form, whether written or electronic) relating or pertaining to this Agreement, including without limitation all ledgers, books, invoices, receipts, vouchers, canceled checks, wage records, timesheets, subcontracts, reports, correspondence, lists, notes, and memoranda, for the duration of this contract or agreement and for at least five (5) years following the completion or termination of this Agreement, including all renewal periods.

2. The OIG designates Kristen Morales as its primary point of contact for all dealings with Contractor related to carrying out this Agreement. All Contractor communications should be directed to Ms. Morales.

F. Audit and Inspection.

1. The Contractor will submit to any City audit, inspection, and review and, at the City's request, will make available all documents relating or pertaining to this Agreement maintained by or under the control of the Contractor, its employees, agents, assigns, successors and subcontractors, during normal business hours at the Contractor's office or place of business in Louisiana. If no such location is available, the Contractor will make the documents available at a

time and location that is convenient for the City.

2. The Contractor will abide by all provisions of City Code § 2-1120, including but not limited to City Code § 2-1120(12), which requires the Contractor to provide the Office of Inspector General with documents and information as requested. Failure to comply with such requests shall constitute a material breach of the contract. The Contractor agrees that it is subject to the jurisdiction of the Orleans Parish Civil District Court for purposes of challenging a subpoena.

G. Insurance.

1. Except as otherwise noted, at all times during this Agreement or the performance of work required by this Agreement, the Contractor will maintain the following insurance in full force and effect for the duration of the work under this Agreement:

1. Commercial General Liability (CGL) Policy # __ 83SBMPW1252 __, written on an “occurrence” basis, including products and completed operations, property damage, bodily injury and personal & advertising injury with limits of \$1,000,000 per occurrence, with a general aggregate limit of \$2,000,000.

2. Workers’ Compensation: as required by the State of Louisiana, with Statutory Limits, and Employer’s Liability Insurance with limit of no less than \$1,000,000 per accident for bodily injury or disease.

Additional Insured Status

Contractor has provided, and will maintain current, a Certificate of Insurance naming the Office of Inspector General and the City of New Orleans as “Additional Insureds” on the CGL policy with respect to liability arising out of the performance of this agreement.

Primary Coverage

For any claims related to this contract, Contractor’s insurance coverage shall be primary insurance in respect to Office of Inspector General and the City of New Orleans. Any insurance or self-insurance maintained by the City shall be non- contributing to Contractor’s coverage.

Waiver of Subrogation

Contractor and its insurers agree to waive any right of subrogation which any insurer may acquire against the City by virtue of the payment of any loss under insurance required by this contract.

Notice of Cancellation

Each insurance policy required above shall provide that coverage shall not be canceled, except with prior notice to the Office of Inspector General of no less than 60 days.

H. Indemnity.

1. The Contractor will indemnify, defend, and hold harmless the City, its agents, employees, officials, insurers, self-insurance funds, and assigns (collectively, the "Indemnified Parties") from and against any and all claims, demands, suits, and judgments of sums of money accruing against the Released Parties: for all liability, costs and expenses arising directly or indirectly out of any act of omission of the Contractor, its agents, subcontractors, or employees or otherwise arising out of the performance of the services pursuant to this Agreement.

2. The Contractor's indemnity does not extend to any loss arising from the gross negligence or willful misconduct of any of the Indemnified Parties, provided that neither the Contractor nor any of its agents, subcontractors, or employees contributed to such gross negligence or willful misconduct.

3. The Contractor has an immediate and independent obligation to, at the City's option: (a) defend the City from or (b) reimburse the City for its costs incurred in the defense of any claim that actually or potentially falls within this indemnity, even if: (a) the allegations are or may be groundless, false, or fraudulent; or (b) the Contractor is ultimately absolved from liability.

II. REPRESENTATIONS AND WARRANTIES.

A. The Contractor represents and warrants to the OIG that:

1. The Contractor, through its duly authorized representative, has the full power and authority to enter into and execute this Agreement;

2. The Contractor has the requisite expertise, qualifications, staff, materials, equipment, licenses, permits, consents, registrations, and certifications in place and available for the performance of all work required under this Agreement;

3. The Contractor is fully and adequately insured for any injury or loss to its employees and any other person resulting from the actions or omissions of the Contractor, or its employees in the performance of this Agreement;

4. The Contractor is not under any obligation to any other person that is inconsistent or in conflict with this Agreement or that could prevent, limit, or impair the Contractor's performance of this Agreement;

5. The Contractor has no knowledge of any facts that could prevent, limit, or impair the performance of this Agreement;

6. The Contractor is not in breach of any federal, state, or local statute or regulation applicable to the Contractor or its operations;

8. The Contractor has read and fully understands this Agreement, including the solicitation, and is executing this Agreement willingly and voluntarily; and

9. All of the representations and warranties in this Article and elsewhere in this

Agreement are true and correct as of the date of this Agreement by the Contractor and the execution of this Agreement by the Contractor's representative constitutes a sworn statement, under penalty of perjury, by the Contractor as to the truth of the foregoing representations and warranties.

B. Convicted Felon Statement. The Contractor complies with City Code § 2-8(c) and no principal, member, or officer of the Contractor has, within the preceding five years, been convicted of, or pled guilty to, a felony under state or federal statutes for embezzlement, theft of public funds, bribery, or falsification or destruction of public records.

C. Non-Solicitation Statement. The Contractor has not employed or retained any company or person, other than a bona fide employee working solely for it, to solicit or secure this Agreement. The Contractor has not paid or agreed to pay any person, other than a bona fide employee working for it, any fee, commission, percentage, gift, or any other consideration contingent upon or resulting from this Agreement.

D. The Contractor acknowledges that the City/OIG is relying on these representations and warranties and Contractor's expertise, skill, and knowledge and that the Contractor's obligations and liabilities will not be diminished by reason of any approval by the City/OIG.

III. THE CITY'S OBLIGATIONS.

A. Administration. The City will:

1. Administer this Agreement through the Office of Inspector General (OIG), which will assign or authorize work under this Agreement;
2. Provide the Contractor any documents deemed necessary for the Contractor's performance of any work required under this Agreement;
3. Provide the Contractor with project oversight;
4. Provide access to OIG personnel to discuss the required services as requested by the Contractor.

B. Payment. The City will make payments to the Contractor at the rate of compensation established in this Agreement within thirty (30) days of the receipt of the Contractor's certified invoices, except:

1. The City's obligation to make any payment is contingent upon the Contractor's: (a) submission of a complete and accurate invoice, including all required information and documents; (b) satisfactory performance of the services and conditions required by this Agreement, including, without limitation, satisfactory deliverables;
2. Unless specifically authorized by a validly executed amendment, the City/OIG is not obligated under any circumstances to pay for any work performed or costs incurred by the Contractor that:
 - a) Exceed the maximum aggregate amount payable established by this Agreement;
 - b) Are beyond the scope or duration of this Agreement;

- c) Arise from or relate to the any change order within the scope of the Agreement;
- d) Arise from or relate to the correction of errors or omissions of the Contractor or its subcontractors; or
- e) The City is not expressly obligated to pay under this Agreement.

3. The OIG, in its discretion, may withhold payment of any disputed amounts, and no interest shall accrue on any amount withheld pending the resolution of the dispute.

4. If this Agreement is terminated for any reason, the City will pay the Contractor only for the work requested by the OIG and satisfactorily performed by the Contractor through the date of termination, except as otherwise provided in this Agreement.

IV. COMPENSATION.

A. Rate of Compensation.

This Agreement does not guarantee any amount of work or compensation except as specifically authorized by the OIG in accordance with the terms and conditions of this Agreement. The stated compensation is inclusive, and includes no additional amounts for the Contractor's costs, including without limitation all expenses relating to overhead, administration, subcontractors, employees, bid preparation, bonds, scheduling, invoicing, insurance, record retention, reporting, inspections, audits, the correction of errors and omissions, or minor changes within the scope of this Agreement.

The Contractor immediately will notify the City in writing of any reduction to the rate of compensation for its most favored customer and the rate of compensation established by this Agreement automatically will adjust to the reduced rate effective as of the effective date of the reduction for the most favored customer.

B. Maximum Amount. The maximum aggregate amount payable by the City under this Agreement is TWENTY-FIVE THOUSAND DOLLARS (\$25,000).

V. DURATION AND TERMINATION.

A. Initial Term. The initial term of this Agreement covers one year from the effective date of the Agreement.

B. Extension. The OIG may extend the term this Agreement for no more than two (2) successive one (1) year periods pursuant to validly executed amendments, provided that:

- 1. Any extension of this Agreement is subject to and contingent upon the encumbrance of funds;
- 2. The OIG determines that the extension facilitates the continuity of services provided under this Agreement; and
- 3. The total duration of the Agreement, including the original term and any extensions, shall not exceed three (3) years.

C. Termination for Convenience. Either party to this Agreement may terminate the agreement at any time during the term of the agreement by giving the other party written notice of said intention to terminate at least thirty (30) calendar days before the intended date of termination.

D. Termination for Non-Appropriation. This Agreement will terminate immediately in the event of non-appropriation of funds sufficient to maintain this Agreement without the requirement of notice.

E. Termination for Cause. The OIG may terminate this Agreement immediately for cause by sending written notice to the Contractor. "Cause" includes without limitation any failure to perform any obligation or abide by any condition of this Agreement or the failure of any representation or warranty in this Agreement, including any failure to comply with the requirements of the City's Disadvantaged Business Enterprise program and any failure to comply with any provision of City Code § 2-1120 or requests of the Office of Inspector General.

F. Suspension. The OIG may suspend this Agreement at any time and for any reason by giving two (2) business day's written notice to the Contractor. The Contractor will resume work upon five (5) business day's written notice from the OIG.

VI. NON-DISCRIMINATION.

A. Equal Employment Opportunity. In all hiring or employment made possible by, or resulting from this Agreement, the Contractor (1) will not be discriminate against any employee or applicant for employment because of race, color, religion, gender, age, physical or mental disability, national origin, sexual orientation, creed, culture, or ancestry, and (2) where applicable, will take affirmative action to ensure that the Contractor's employees are treated during employment without regard to their race, color, religion, gender, age, physical or mental disability, national origin, sexual orientation, creed, culture, or ancestry. This requirement shall apply to, but not be limited to the following: employment, upgrading, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship. All solicitations or advertisements for employees shall state that all qualified applicants will receive consideration for employment without regard to race, color, religion, gender, age, physical or mental disability, national origin, sexual orientation, creed, culture, or ancestry.

B. Non-Discrimination. In the performance of this Agreement, the Contractor will not discriminate on the basis, whether in fact or perception, of a person's race, color, creed, religion, national origin, ancestry, age, sex (gender), sexual orientation, gender identity, domestic partner status, marital status, physical or mental disability, or AIDS- or HIV-status against (1) any employee of the City working with the Contractor in any of Contractor's operations within Orleans Parish or (2) any person seeking accommodations, advantages, facilities, privileges, services, or membership in all business, social, or other establishments or organizations operated by the Contractor. The Contractor agrees to comply with and abide by all applicable federal, state and local laws relating to non-discrimination, including, without limitation, Title VI of the Civil Rights Act of 1964, Section V of the Rehabilitation Act of 1973,

and the Americans with Disabilities Act of 1990.

C. The OIG may terminate this Agreement for cause if the Contractor fails to comply with any obligation in this Article, which failure is a material breach of this Agreement.

VII. INDEPENDENT CONTRACTOR.

A. **Independent Contractor Status.** The Contractor is an independent contractor and shall not be deemed an employee, servant, agent, partner, or joint venture of the City and will not hold itself or any of its employees, subcontractors or agents to be an employee, partner, or agent of the City.

B. **Exclusion of Worker's Compensation Coverage.** The City will not be liable to the Contractor, as an independent contractor as defined in La. R.S. 23:1021(6), for any benefits or coverage as provided by the Workmen's Compensation Law of the State of Louisiana. Under the provisions of La. R.S. 23:1034, any person employed by the Contractor will not be considered an employee of the City for the purpose of Worker's Compensation coverage.

C. **Exclusion of Unemployment Compensation Coverage.** The Contractor, as an independent contractor, is being hired by the City under this Agreement for hire and defined in La. R.S. 23:1472(E) and neither the Contractor nor anyone employed by it will be considered an employee of the City for the purpose of unemployment compensation coverage, which coverage same being hereby expressly waived and excluded by the parties, because: (a) the Contractor has been and will be free from any control or direction by the City over the performance of the services covered by this contract; (b) the services to be performed by the Contractor are outside the normal course and scope of the City's usual business; and (c) the Contractor has been independently engaged in performing the services required under this Agreement prior to the date of this Agreement.

D. **Waiver of Benefits.** The Contractor, as an independent contractor, will not receive from the City any sick and annual leave benefits, medical insurance, life insurance, paid vacations, paid holidays, sick leave, pension, or Social Security for any services rendered to the City under this Agreement.

VIII. NOTICE.

A. **Notice Requirements.** Any notice, demand, communication or request required or permitted under this Agreement (except for any routine communications) shall be in writing and delivered in person or by certified mail, return receipt requested, as follows:

i. To the OIG:

Office of Inspector General for the City of New Orleans
Suzanne Lacey Wisdom
525 St. Charles Avenue
New Orleans, LA 70130

To the City:
City Attorney
City of New Orleans
1300 Perdido St. 5E03
New Orleans, LA 70112

- ii. To the Contractor:
Ultimate Technical Solutions, Inc.
Attn: David St. Etienne
651 Leson Ct.
Harvey, LA 70058

All changes of address or recipient(s) must be provided to each party in a writing that specifically identifies this Agreement. Nothing contained in this Article shall be construed to restrict the transmission of routine communications between representatives of OIG and the Contractor.

B. Receipt of Notices. Notices are effective upon receipt at the address specified above. Any notice sent but not received by or delivered to the intended recipient because of any refusal or evasion of delivery shall be deemed effective on the date of the first attempted delivery.

IX. ADDITIONAL PROVISIONS.

A. Limitations of the City's Obligations. The City has no obligations not explicitly set forth in this Agreement or any incorporated documents or expressly imposed by law.

B. No Promotional Content. The OIG website will not contain any content promoting or advertising the Contractor.

C. Ownership Interest Disclosure. The Contractor will provide a sworn affidavit listing all natural or artificial persons with an ownership interest in the Contractor and stating that no other person holds an ownership interest in the Contractor via a counter letter. For the purposes of this provision, an "ownership interest" shall not be deemed to include ownership of stock in a publicly traded corporation or ownership of an interest in a mutual fund or trust that holds an interest in a publicly traded corporation. If the Contractor fails to submit the required affidavits, the OIG may, after 30 days' written notice to the Contractor, take such action as may be necessary to cause the suspension of any further payments until such the required affidavits are submitted.

D. No Subcontractors. No subcontractors are permitted under this contract.

E. Prohibition of Financial Interest in Agreement. No elected official or employee of the City shall have a financial interest, direct or indirect, in this Agreement. For purposes of this provision, a financial interest held by the spouse, child, or parent of any elected official or

employee of the City shall be deemed to be a financial interest of such elected official or employee of the City. Any willful violation of this provision, with the expressed or implied knowledge of Contractor, shall render this Agreement voidable by the City and shall entitle the City to recover, in addition to any other rights and remedies available to the City, all monies paid by the City to Contractor pursuant to this Agreement without regard to Contractor's otherwise satisfactory performance of the Agreement.

F. Prohibition on Political Activity. None of the funds, materials, property, or services provided directly or indirectly under the terms of this Agreement shall be used in the performance of this Agreement for any partisan political activity, or to further the election or defeat of any candidate for public office.

G. Conflicting Employment. To ensure that the Contractor's efforts do not conflict with the City's interests, and in recognition of the Contractor's obligations to the OIG, the Contractor will decline any offer of other employment if its performance of this Agreement is likely to be adversely affected by the acceptance of the other employment. The Contractor will promptly notify the OIG in writing of its intention to accept the other employment and will disclose all possible effects of the other employment on the Contractor's performance of this Agreement. The OIG will make the final determination whether the Contractor may accept the other employment.

H. Non-Exclusivity. This Agreement is non-exclusive and the Contractor may provide services to other clients, subject to the OIG's approval of any potential conflicts with the performance of this Agreement and the City may engage the services of others for the provision of some or all of the work to be performed under this Agreement.

I. Assignment. This Agreement and any part of the Contractor's interest in it are not assignable or transferable without the OIG's prior written consent.

J. Terms Binding. The terms and conditions of this Agreement are binding on any heirs, successors, transferees, and assigns.

K. Jurisdiction. The Contractor consents and yields to the jurisdiction of the State Civil Courts of the Parish of Orleans and formally waives any pleas or exceptions of jurisdiction on account of the residence of the Contractor.

L. Choice of Law. This Agreement will be construed and enforced in accordance with the laws of the State of Louisiana without regard to its conflict of laws provisions.

M. Construction of Agreement. Neither party will be deemed to have drafted this Agreement. This Agreement has been reviewed by all parties and shall be construed and interpreted according to the ordinary meaning of the words used so as to fairly accomplish the purposes and intentions of all parties. No term of this Agreement shall be construed or resolved in favor of or against the City or the Contractor on the basis of which party drafted the uncertain or ambiguous language. The headings and captions of this Agreement are provided for convenience only and are not intended to have effect in the construction or interpretation of this Agreement. Where appropriate, the singular includes the plural and neutral words and

words of any gender shall include the neutral and other gender.

N. Severability. Should a court of competent jurisdiction find any provision of this Agreement to be unenforceable as written, the unenforceable provision should be reformed, if possible, so that it is enforceable to the maximum extent permitted by law or, if reformation is not possible, the unenforceable provision shall be fully severable and the remaining provisions of the Agreement remain in full force and effect and shall be construed and enforced as if the unenforceable provision was never a part the Agreement.

O. Survival of Certain Provisions. All representations and warranties and all obligations concerning record retention, inspections, audits, ownership, indemnification, payment, remedies, jurisdiction, and choice of law shall survive the expiration, suspension, or termination of this Agreement and continue in full force and effect.

P. No Third Party Beneficiaries. This Agreement is entered into for the exclusive benefit of the parties and the parties expressly disclaim any intent to benefit anyone not a party to this Agreement.

Q. Amendment. No amendment of or modification to this Agreement shall be valid unless and until executed in writing by the duly authorized representatives of both parties to this Agreement.

R. Non-Waiver. The failure of either party to insist upon strict compliance with any provision of this Agreement, to enforce any right or to seek any remedy upon discovery of any default or breach of the other party at such time as the initial discovery of the existence of such noncompliance, right, default or breach shall not affect or constitute a waiver of either party's right to insist upon such compliance, exercise such right or seek such remedy with respect to that default or breach or any prior contemporaneous or subsequent default or breach.

S. Entire Agreement. This Agreement, including all incorporated documents, constitutes the final and complete agreement and understanding between the parties. All prior and contemporaneous agreements and understandings, whether oral or written, are superseded by this Agreement and are without effect to vary or alter any terms or conditions of this Agreement.

SIGNATURES ON FOLLOWING PAGE:

IN WITNESS WHEREOF, the City and the Contractor execute this Agreement.

CITY OF NEW ORLEANS

BY: _____

MITCHELL J. LANDRIEU, MAYOR

9/21/15

FORM AND LEGALITY APPROVED:

Law Department

By: _____

Printed Name: _____

John P. Meng

ULTIMATE TECHNICAL SOLUTIONS, INC.:

BY: _____

DAVID ST. ETIENNE, PRESIDENT/CEO

Tax ID No. 72-1039480

ATTACHMENT I: FEE PROPOSAL/KEY PERSONNEL

- The hourly fees in this proposal include all company overhead, profit, and costs.
- Expenses are not allowable under this contract and may not be billed to the OIG.
- Travel time to/from on-site visits or any other travel required by the contract shall not be billed to the OIG.
- All consultant time will be billed in increments of 1/10 hour.
- Electronic communications will not be billed unless the content of the consultant's single response exceeds 500 words.
- All time billed will be detailed by date and time entry on the invoice with a description of the service provided, including whether the service was via email, telephone, remote access, or on-site.
- Invoices will be sent to the OIG at least monthly or more frequently if the total amount of an invoice exceeds \$1,000.
- The company may not bill for more than one consultant to attend any meeting or provide any service unless the OIG gives advance written approval.

Primary Consultant Shaun Covey **Hourly Rate \$** 67.00

Other consultants who may provide services:

Name Darren Goodridge Hourly Rate \$ 67.00

Name Edward Gabriel Hourly Rate \$ 67.00

Name Scot Guelfo Hourly Rate \$ 67.00

Please attach resumes for every person listed on this form.

ATTACHMENT II

Office of Inspector General for the City of New Orleans Information Technology and Information Systems Rules of Behavior and Confidentiality Agreement

Purpose: This agreement outlines the acceptable and unacceptable uses of OIG Information Technology (IT) and Information Systems (IS). It also outlines the signer's responsibilities regarding stewardship and use of OIG IT/IS.

Scope: This agreement applies to anyone granted access to any OIG IT/IS, including but not limited to OIG employees, contractors and interns. All references to IT/IS monitoring herein pertain to data communications only (emails, facsimile, computer database use and data storage, digital transmission of data, etc.) and not to voice communications. This agreement form must be signed before access to any OIG IT/IS is granted.

Statement of Responsibility: I understand that I am to use OIG systems for lawful, official use and authorized purposes as further outlined in this document and other OIG policy directives. Even where granted access, I must only access the system files and information on a need-to-know basis and only in furtherance of authorized tasks or mission-related functions.

General. I am responsible for all activity on any OIG IS that is authorized to operate in OIG space and that occurs on my individual account(s) once my logon credential or password has been used to logon. If I am a member of a "group account," I am responsible for all of my activity when I am logged on an IS associated with that account.

I am responsible for all IT that I introduce into OIG approved space including devices that are privately owned, or those owned by another government agency. I understand that I must obtain written permission to introduce any non-OIG hardware, software, or media into OIG controlled space, and that I may not use non-OIG hardware, software, or media to connect to or communicate with any OIG system without authorization from the OIG.

I acknowledge that the ultimate responsibility for ensuring the protection of OIG non-public information lies with me, the user of OIG IT/IS and non-OIG IT/IS authorized to operate in OIG spaces.

Revocability: The ability to use IT in OIG space and access to OIG IT/IS is a revocable privilege.

Rules of Behavior: I will adhere to the following Rules of Behavior (ROB):

1. I consent to monitoring or search of any IT/IS equipment or media I bring into, or remove from, OIG owned, controlled or leased facilities. When asked by authorized personnel I will provide unfettered access to all equipment or media brought into or removed from such OIG facilities. I also understand that OIG or OIG leased IS may be monitored or otherwise accessed

for law enforcement or other compliance purposes and my agreement to this OIG ROB constitutes my consent to be monitored and to allow access to OIG IS accessed by me.

2. I will:

- a. Use only properly licensed OIG approved software and hardware.
- b. Protect all copyright and other intellectual property rights according to terms and conditions contained in OIG approved software and hardware licenses.
- c. Use OIG IT equipment, including but not limited to portable electronic devices (PED) and keyboard, video, monitor (KVM) switch devices, according to and in compliance with OIG policy directives.
- d. Use OIG computer and network applications and systems, including but not limited to, email, databases, and web services according to and in compliance with OIG policy directives.
- e. Use OIG embedded and add-on peripheral devices including cameras, microphones, and storage devices according to and in compliance with OIG policy directives.

3. When using OIG IT/IS, I will:

- a. Use strong passwords, and agree to change my password with a frequency as specified by policy or as requested for security reasons.
- b. Protect my password(s) from disclosure to other people.
- c. Use screen locks or logoff my workstation upon departing the immediate area.
- d. Use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.
- e. Use only authorized media (thumb drives, diskettes, etc) and procedures to download or store OIG information.
- f. Disseminate any OIG non-public information only to OIG IT Specialist.
- i. Destroy copies and extracts of sensitive data that are no longer needed using OIG approved destruction procedures.

4. I will immediately report known or suspected security incidents or improper use of OIG IT/IS to the OIG IT Specialist upon discovery regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information.

5. I will read and understand the network warning banner that is presented prior to network log on. I will address any questions regarding that banner to the OIG IT Specialist.

Expressly Prohibited Behavior: I will **NOT** conduct or participate in any of the following behaviors or activities on any OIG IT, IS. I will not:

1. Knowingly violate any statute or order, such as compliance legislation, copyright laws, or laws governing disclosure of information, including but not limited to:
 - a. Connect classified IT/IS to the Internet or other unclassified systems.
 - b. Remove sensitive/classified media (paper or electronic) from OIG offices.
-

c. Use OIG IT/IS or OIG non-public information for personal benefit, profit, to benefit other persons, non-profit business dealings, any political (e.g., lobbying or campaigning) party candidate or issue or for any illegal activity.

2. Misuse my OIG IT/IS privileges including:

- a. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).
- b. Permit any unauthorized person access to OIG systems.
- c. Use an account, user ID, or password not specifically assigned to me, masquerade as another user, or otherwise misrepresent my identity and privileges to IT/IS administrators and security personnel.

3. Exhibit behavior that could lead to damage, endangerment or degradation of OIG equipment, software, media, data, facilities, services, or people, including but not limited to:

- a. Attempt to circumvent access controls or to use unauthorized means (e.g., penetration testing, password cracking, "sniffer" programs), to gain access to accounts, files, folders or data on OIG IT/IS.
- b. Change configuration settings of operating systems or security related software, or security related information. Nor will I remove, modify, or add any hardware or software to/from OIG IT/IS without approval of my ISSO.
- c. Tamper (e.g., alter, change, configure, install software or hardware, or connect IT or systems) with my computer to circumvent any OIG policy and IT/IS protections.
- d. Open e-mails or other messages from suspicious sources (e.g., sources that you do not recognize as legitimate).
- e. Visit untrustworthy or inappropriate Web sites. For example, I will pay careful attention to the Universal Resource Locator (URL) of a web site inasmuch as URLs for malicious or untrustworthy web sites may look identical to a legitimate web site, but the URL may use a variation in spelling or a different domain (e.g., .com instead of net; or .com in place of .gov).
- f. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).
- g. Create or intentionally spread malicious code (i.e. viruses and Trojans).
- h. Attempt to access any security audit trail information that may exist without authorization.
- i. Install or connect non-OIG owned or leased (including privately owned) software or hardware (e.g., PEDS, such as Palm Pilots, Blackberrys, MP3 Players...etc.) and removable media (e.g., thumb drives, memory sticks...etc.) to OIG IT/IS.
- j. Introduce wireless devices into OIG space without authorization from the OIG IT Specialist.

4. Participate in prohibited activities, including but not limited to:

- a. Download, view, or send pornography or obscene material.
 - b. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.
 - c. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional according to OIG standards of professional behavior.
 - d. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.
-

- e. Use internet "chat" services (e.g., AOL, Instant Messenger (IM), Microsoft Network IM, Yahoo IM...etc).
- f. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
- g. "Surf" through OIG files containing personal information merely for personal curiosity.
- h. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.)

Confidentiality

All material, records, data, and information which may become available to Contractor in carrying out this Agreement are confidential and must be protected from disclosure. Contractor acknowledges a duty to protect all such material, records, data, and information and understands that unauthorized disclosure of confidential records or information may constitute a misdemeanor punishable, pursuant to La. R.S. 33:9614, by a fine of not more than two thousand dollars or imprisonment for not more than one year, or both. In addition, all proprietary information relating to the OIG or IPM computer networks, including but not limited to security access codes and security features, are confidential and Contractor must protect such information from disclosure.

Acknowledgment

I acknowledge that I have read and understand the above listed Rules of Behavior. I also state that I will adhere to these Rules of Behavior and that failure to do so may constitute a security violation resulting in denial of access to OIG IT/IS networks or facilities. I also understand that violation of these rules of behavior will be reported to the appropriate authorities and may result in administrative, criminal, or other adverse disciplinary action deemed appropriate.

Printed Name: Shawn Corey Date: 9/15/15

Employee Signature:  Last Four of SSN: xxx-xx-4244

ATTACHMENT II
Office of Inspector General for the City of New Orleans
Information Technology and Information Systems
Rules of Behavior and Confidentiality Agreement

Purpose: This agreement outlines the acceptable and unacceptable uses of OIG Information Technology (IT) and Information Systems (IS). It also outlines the signer's responsibilities regarding stewardship and use of OIG IT/IS.

Scope: This agreement applies to anyone granted access to any OIG IT/IS, including but not limited to OIG employees, contractors and interns. All references to IT/IS monitoring herein pertain to data communications only (emails, facsimile, computer database use and data storage, digital transmission of data, etc.) and not to voice communications. This agreement form must be signed before access to any OIG IT/IS is granted.

Statement of Responsibility: I understand that I am to use OIG systems for lawful, official use and authorized purposes as further outlined in this document and other OIG policy directives. Even where granted access, I must only access the system files and information on a need-to-know basis and only in furtherance of authorized tasks or mission-related functions.

General. I am responsible for all activity on any OIG IS that is authorized to operate in OIG space and that occurs on my individual account(s) once my logon credential or password has been used to logon. If I am a member of a "group account," I am responsible for all of my activity when I am logged on an IS associated with that account.

I am responsible for all IT that I introduce into OIG approved space including devices that are privately owned, or those owned by another government agency. I understand that I must obtain written permission to introduce any non-OIG hardware, software, or media into OIG controlled space, and that I may not use non-OIG hardware, software, or media to connect to or communicate with any OIG system without authorization from the OIG.

I acknowledge that the ultimate responsibility for ensuring the protection of OIG non-public information lies with me, the user of OIG IT/IS and non-OIG IT/IS authorized to operate in OIG spaces.

Revocability: The ability to use IT in OIG space and access to OIG IT/IS is a revocable privilege.

Rules of Behavior: I will adhere to the following Rules of Behavior (ROB):

1. I consent to monitoring or search of any IT/IS equipment or media I bring into, or remove from, OIG owned, controlled or leased facilities. When asked by authorized personnel I will provide unfettered access to all equipment or media brought into or removed from such OIG facilities. I also understand that OIG or OIG leased IS may be monitored or otherwise accessed

for law enforcement or other compliance purposes and my agreement to this OIG ROB constitutes my consent to be monitored and to allow access to OIG IS accessed by me.

2. I will:

- a. Use only properly licensed OIG approved software and hardware.
- b. Protect all copyright and other intellectual property rights according to terms and conditions contained in OIG approved software and hardware licenses.
- c. Use OIG IT equipment, including but not limited to portable electronic devices (PED) and keyboard, video, monitor (KVM) switch devices, according to and in compliance with OIG policy directives.
- d. Use OIG computer and network applications and systems, including but not limited to, email, databases, and web services according to and in compliance with OIG policy directives.
- e. Use OIG embedded and add-on peripheral devices including cameras, microphones, and storage devices according to and in compliance with OIG policy directives.

3. When using OIG IT/IS, I will:

- a. Use strong passwords, and agree to change my password with a frequency as specified by policy or as requested for security reasons.
- b. Protect my password(s) from disclosure to other people.
- c. Use screen locks or logoff my workstation upon departing the immediate area.
- d. Use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.
- e. Use only authorized media (thumb drives, diskettes, etc) and procedures to download or store OIG information.
- f. Disseminate any OIG non-public information only to OIG IT Specialist.
- i. Destroy copies and extracts of sensitive data that are no longer needed using OIG approved destruction procedures.

4. I will immediately report known or suspected security incidents or improper use of OIG IT/IS to the OIG IT Specialist upon discovery regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information.

5. I will read and understand the network warning banner that is presented prior to network log on. I will address any questions regarding that banner to the OIG IT Specialist.

Expressly Prohibited Behavior: I will **NOT** conduct or participate in any of the following behaviors or activities on any OIG IT, IS. I will not:

1. Knowingly violate any statute or order, such as compliance legislation, copyright laws, or laws governing disclosure of information, including but not limited to:
 - a. Connect classified IT/IS to the Internet or other unclassified systems.
 - b. Remove sensitive/classified media (paper or electronic) from OIG offices.
-

c. Use OIG IT/IS or OIG non-public information for personal benefit, profit, to benefit other persons, non-profit business dealings, any political (e.g., lobbying or campaigning) party candidate or issue or for any illegal activity.

2. Misuse my OIG IT/IS privileges including:

- a. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).
- b. Permit any unauthorized person access to OIG systems.
- c. Use an account, user ID, or password not specifically assigned to me, masquerade as another user, or otherwise misrepresent my identity and privileges to IT/IS administrators and security personnel.

3. Exhibit behavior that could lead to damage, endangerment or degradation of OIG equipment, software, media, data, facilities, services, or people, including but not limited to:

- a. Attempt to circumvent access controls or to use unauthorized means (e.g., penetration testing, password cracking, "sniffer" programs), to gain access to accounts, files, folders or data on OIG IT/IS.
- b. Change configuration settings of operating systems or security related software, or security related information. Nor will I remove, modify, or add any hardware or software to/from OIG IT/IS without approval of my ISSO.
- c. Tamper (e.g., alter, change, configure, install software or hardware, or connect IT or systems) with my computer to circumvent any OIG policy and IT/IS protections.
- d. Open e-mails or other messages from suspicious sources (e.g., sources that you do not recognize as legitimate).
- e. Visit untrustworthy or inappropriate Web sites. For example, I will pay careful attention to the Universal Resource Locator (URL) of a web site inasmuch as URLs for malicious or untrustworthy web sites may look identical to a legitimate web site, but the URL may use a variation in spelling or a different domain (e.g., .com instead of net; or .com in place of .gov).
- f. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).
- g. Create or intentionally spread malicious code (i.e. viruses and Trojans).
- h. Attempt to access any security audit trail information that may exist without authorization.
- i. Install or connect non-OIG owned or leased (including privately owned) software or hardware (e.g., PEDS, such as Palm Pilots, Blackberrys, MP3 Players...etc.) and removable media (e.g., thumb drives, memory sticks...etc.) to OIG IT/IS.
- j. Introduce wireless devices into OIG space without authorization from the OIG IT Specialist.

4. Participate in prohibited activities, including but not limited to:

- a. Download, view, or send pornography or obscene material.
 - b. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.
 - c. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional according to OIG standards of professional behavior.
 - d. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.
-

- e. Use internet "chat" services (e.g., AOL, Instant Messenger (IM), Microsoft Network IM, Yahoo IM...etc).
- f. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
- g. "Surf" through OIG files containing personal information merely for personal curiosity.
- h. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.)

Confidentiality

All material, records, data, and information which may become available to Contractor in carrying out this Agreement are confidential and must be protected from disclosure. Contractor acknowledges a duty to protect all such material, records, data, and information and understands that unauthorized disclosure of confidential records or information may constitute a misdemeanor punishable, pursuant to La. R.S. 33:9614, by a fine of not more than two thousand dollars or imprisonment for not more than one year, or both. In addition, all proprietary information relating to the OIG or IPM computer networks, including but not limited to security access codes and security features, are confidential and Contractor must protect such information from disclosure.

Acknowledgment

I acknowledge that I have read and understand the above listed Rules of Behavior. I also state that I will adhere to these Rules of Behavior and that failure to do so may constitute a security violation resulting in denial of access to OIG IT/IS networks or facilities. I also understand that violation of these rules of behavior will be reported to the appropriate authorities and may result in administrative, criminal, or other adverse disciplinary action deemed appropriate.

Printed Name: Scot Guetta Date: 9/15/15

Employee Signature:  Last Four of SSN: xxx-xx-7719

ATTACHMENT II

Office of Inspector General for the City of New Orleans Information Technology and Information Systems Rules of Behavior and Confidentiality Agreement

Purpose: This agreement outlines the acceptable and unacceptable uses of OIG Information Technology (IT) and Information Systems (IS). It also outlines the signer's responsibilities regarding stewardship and use of OIG IT/IS.

Scope: This agreement applies to anyone granted access to any OIG IT/IS, including but not limited to OIG employees, contractors and interns. All references to IT/IS monitoring herein pertain to data communications only (emails, facsimile, computer database use and data storage, digital transmission of data, etc.) and not to voice communications. This agreement form must be signed before access to any OIG IT/IS is granted.

Statement of Responsibility: I understand that I am to use OIG systems for lawful, official use and authorized purposes as further outlined in this document and other OIG policy directives. Even where granted access, I must only access the system files and information on a need-to-know basis and only in furtherance of authorized tasks or mission-related functions.

General. I am responsible for all activity on any OIG IS that is authorized to operate in OIG space and that occurs on my individual account(s) once my logon credential or password has been used to logon. If I am a member of a "group account," I am responsible for all of my activity when I am logged on an IS associated with that account.

I am responsible for all IT that I introduce into OIG approved space including devices that are privately owned, or those owned by another government agency. I understand that I must obtain written permission to introduce any non-OIG hardware, software, or media into OIG controlled space, and that I may not use non-OIG hardware, software, or media to connect to or communicate with any OIG system without authorization from the OIG.

I acknowledge that the ultimate responsibility for ensuring the protection of OIG non-public information lies with me, the user of OIG IT/IS and non-OIG IT/IS authorized to operate in OIG spaces.

Revocability: The ability to use IT in OIG space and access to OIG IT/IS is a revocable privilege.

Rules of Behavior: I will adhere to the following Rules of Behavior (ROB):

1. I consent to monitoring or search of any IT/IS equipment or media I bring into, or remove from, OIG owned, controlled or leased facilities. When asked by authorized personnel I will provide unfettered access to all equipment or media brought into or removed from such OIG facilities. I also understand that OIG or OIG leased IS may be monitored or otherwise accessed

for law enforcement or other compliance purposes and my agreement to this OIG ROB constitutes my consent to be monitored and to allow access to OIG IS accessed by me.

2. I will:

- a. Use only properly licensed OIG approved software and hardware.
- b. Protect all copyright and other intellectual property rights according to terms and conditions contained in OIG approved software and hardware licenses.
- c. Use OIG IT equipment, including but not limited to portable electronic devices (PED) and keyboard, video, monitor (KVM) switch devices, according to and in compliance with OIG policy directives.
- d. Use OIG computer and network applications and systems, including but not limited to, email, databases, and web services according to and in compliance with OIG policy directives.
- e. Use OIG embedded and add-on peripheral devices including cameras, microphones, and storage devices according to and in compliance with OIG policy directives.

3. When using OIG IT/IS, I will:

- a. Use strong passwords, and agree to change my password with a frequency as specified by policy or as requested for security reasons.
- b. Protect my password(s) from disclosure to other people.
- c. Use screen locks or logoff my workstation upon departing the immediate area.
- d. Use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.
- e. Use only authorized media (thumb drives, diskettes, etc) and procedures to download or store OIG information.
- f. Disseminate any OIG non-public information only to OIG IT Specialist.
- i. Destroy copies and extracts of sensitive data that are no longer needed using OIG approved destruction procedures.

4. I will immediately report known or suspected security incidents or improper use of OIG IT/IS to the OIG IT Specialist upon discovery regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information.

5. I will read and understand the network warning banner that is presented prior to network log on. I will address any questions regarding that banner to the OIG IT Specialist.

Expressly Prohibited Behavior: I will **NOT** conduct or participate in any of the following behaviors or activities on any OIG IT, IS. I will not:

1. Knowingly violate any statute or order, such as compliance legislation, copyright laws, or laws governing disclosure of information, including but not limited to:
 - a. Connect classified IT/IS to the Internet or other unclassified systems.
 - b. Remove sensitive/classified media (paper or electronic) from OIG offices.
-

c. Use OIG IT/IS or OIG non-public information for personal benefit, profit, to benefit other persons, non-profit business dealings, any political (e.g., lobbying or campaigning) party candidate or issue or for any illegal activity.

2. Misuse my OIG IT/IS privileges including:

a. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).

b. Permit any unauthorized person access to OIG systems.

c. Use an account, user ID, or password not specifically assigned to me, masquerade as another user, or otherwise misrepresent my identity and privileges to IT/IS administrators and security personnel.

3. Exhibit behavior that could lead to damage, endangerment or degradation of OIG equipment, software, media, data, facilities, services, or people, including but not limited to:

a. Attempt to circumvent access controls or to use unauthorized means (e.g., penetration testing, password cracking, "sniffer" programs), to gain access to accounts, files, folders or data on OIG IT/IS.

b. Change configuration settings of operating systems or security related software, or security related information. Nor will I remove, modify, or add any hardware or software to/from OIG IT/IS without approval of my ISSO.

c. Tamper (e.g., alter, change, configure, install software or hardware, or connect IT or systems) with my computer to circumvent any OIG policy and IT/IS protections.

d. Open e-mails or other messages from suspicious sources (e.g., sources that you do not recognize as legitimate).

e. Visit untrustworthy or inappropriate Web sites. For example, I will pay careful attention to the Universal Resource Locator (URL) of a web site inasmuch as URLs for malicious or untrustworthy web sites may look identical to a legitimate web site, but the URL may use a variation in spelling or a different domain (e.g., .com instead of net; or .com in place of .gov).

f. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).

g. Create or intentionally spread malicious code (i.e. viruses and Trojans).

h. Attempt to access any security audit trail information that may exist without authorization.

i. Install or connect non-OIG owned or leased (including privately owned) software or hardware (e.g., PEDS, such as Palm Pilots, Blackberrys, MP3 Players...etc.) and removable media (e.g., thumb drives, memory sticks...etc.) to OIG IT/IS.

j. Introduce wireless devices into OIG space without authorization from the OIG IT Specialist.

4. Participate in prohibited activities, including but not limited to:

a. Download, view, or send pornography or obscene material.

b. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.

c. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional according to OIG standards of professional behavior.

d. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.

- e. Use internet "chat" services (e.g., AOL, Instant Messenger (IM), Microsoft Network IM, Yahoo IM...etc).
- f. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
- g. "Surf" through OIG files containing personal information merely for personal curiosity.
- h. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.)

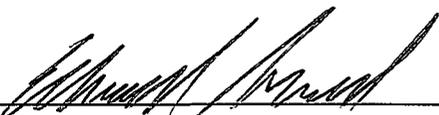
Confidentiality

All material, records, data, and information which may become available to Contractor in carrying out this Agreement are confidential and must be protected from disclosure. Contractor acknowledges a duty to protect all such material, records, data, and information and understands that unauthorized disclosure of confidential records or information may constitute a misdemeanor punishable, pursuant to La. R.S. 33:9614, by a fine of not more than two thousand dollars or imprisonment for not more than one year, or both. In addition, all proprietary information relating to the OIG or IPM computer networks, including but not limited to security access codes and security features, are confidential and Contractor must protect such information from disclosure.

Acknowledgment

I acknowledge that I have read and understand the above listed Rules of Behavior. I also state that I will adhere to these Rules of Behavior and that failure to do so may constitute a security violation resulting in denial of access to OIG IT/IS networks or facilities. I also understand that violation of these rules of behavior will be reported to the appropriate authorities and may result in administrative, criminal, or other adverse disciplinary action deemed appropriate.

Printed Name: EDWARD GABRIEL Date: 9/19/15

Employee Signature:  Last Four of SSN: xxx-xx- 8081

ATTACHMENT II

Office of Inspector General for the City of New Orleans Information Technology and Information Systems Rules of Behavior and Confidentiality Agreement

Purpose: This agreement outlines the acceptable and unacceptable uses of OIG Information Technology (IT) and Information Systems (IS). It also outlines the signer's responsibilities regarding stewardship and use of OIG IT/IS.

Scope: This agreement applies to anyone granted access to any OIG IT/IS, including but not limited to OIG employees, contractors and interns. All references to IT/IS monitoring herein pertain to data communications only (emails, facsimile, computer database use and data storage, digital transmission of data, etc.) and not to voice communications. This agreement form must be signed before access to any OIG IT/IS is granted.

Statement of Responsibility: I understand that I am to use OIG systems for lawful, official use and authorized purposes as further outlined in this document and other OIG policy directives. Even where granted access, I must only access the system files and information on a need-to-know basis and only in furtherance of authorized tasks or mission-related functions.

General. I am responsible for all activity on any OIG IS that is authorized to operate in OIG space and that occurs on my individual account(s) once my logon credential or password has been used to logon. If I am a member of a "group account," I am responsible for all of my activity when I am logged on an IS associated with that account.

I am responsible for all IT that I introduce into OIG approved space including devices that are privately owned, or those owned by another government agency. I understand that I must obtain written permission to introduce any non-OIG hardware, software, or media into OIG controlled space, and that I may not use non-OIG hardware, software, or media to connect to or communicate with any OIG system without authorization from the OIG.

I acknowledge that the ultimate responsibility for ensuring the protection of OIG non-public information lies with me, the user of OIG IT/IS and non-OIG IT/IS authorized to operate in OIG spaces.

Revocability: The ability to use IT in OIG space and access to OIG IT/IS is a revocable privilege.

Rules of Behavior: I will adhere to the following Rules of Behavior (ROB):

1. I consent to monitoring or search of any IT/IS equipment or media I bring into, or remove from, OIG owned, controlled or leased facilities. When asked by authorized personnel I will provide unfettered access to all equipment or media brought into or removed from such OIG facilities. I also understand that OIG or OIG leased IS may be monitored or otherwise accessed
-

for law enforcement or other compliance purposes and my agreement to this OIG ROB constitutes my consent to be monitored and to allow access to OIG IS accessed by me.

2. I will:

- a. Use only properly licensed OIG approved software and hardware.
- b. Protect all copyright and other intellectual property rights according to terms and conditions contained in OIG approved software and hardware licenses.
- c. Use OIG IT equipment, including but not limited to portable electronic devices (PED) and keyboard, video, monitor (KVM) switch devices, according to and in compliance with OIG policy directives.
- d. Use OIG computer and network applications and systems, including but not limited to, email, databases, and web services according to and in compliance with OIG policy directives.
- e. Use OIG embedded and add-on peripheral devices including cameras, microphones, and storage devices according to and in compliance with OIG policy directives.

3. When using OIG IT/IS, I will:

- a. Use strong passwords, and agree to change my password with a frequency as specified by policy or as requested for security reasons.
- b. Protect my password(s) from disclosure to other people.
- c. Use screen locks or logoff my workstation upon departing the immediate area.
- d. Use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.
- e. Use only authorized media (thumb drives, diskettes, etc) and procedures to download or store OIG information.
- f. Disseminate any OIG non-public information only to OIG IT Specialist.
- i. Destroy copies and extracts of sensitive data that are no longer needed using OIG approved destruction procedures.

4. I will immediately report known or suspected security incidents or improper use of OIG IT/IS to the OIG IT Specialist upon discovery regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information.

5. I will read and understand the network warning banner that is presented prior to network log on. I will address any questions regarding that banner to the OIG IT Specialist.

Expressly Prohibited Behavior: I will **NOT** conduct or participate in any of the following behaviors or activities on any OIG IT, IS. I will not:

1. Knowingly violate any statute or order, such as compliance legislation, copyright laws, or laws governing disclosure of information, including but not limited to:
 - a. Connect classified IT/IS to the Internet or other unclassified systems.
 - b. Remove sensitive/classified media (paper or electronic) from OIG offices.
-

c. Use OIG IT/IS or OIG non-public information for personal benefit, profit, to benefit other persons, non-profit business dealings, any political (e.g., lobbying or campaigning) party candidate or issue or for any illegal activity.

2. Misuse my OIG IT/IS privileges including:

- a. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).
- b. Permit any unauthorized person access to OIG systems.
- c. Use an account, user ID, or password not specifically assigned to me, masquerade as another user, or otherwise misrepresent my identity and privileges to IT/IS administrators and security personnel.

3. Exhibit behavior that could lead to damage, endangerment or degradation of OIG equipment, software, media, data, facilities, services, or people, including but not limited to:

- a. Attempt to circumvent access controls or to use unauthorized means (e.g., penetration testing, password cracking, "sniffer" programs), to gain access to accounts, files, folders or data on OIG IT/IS.
- b. Change configuration settings of operating systems or security related software, or security related information. Nor will I remove, modify, or add any hardware or software to/from OIG IT/IS without approval of my ISSO.
- c. Tamper (e.g., alter, change, configure, install software or hardware, or connect IT or systems) with my computer to circumvent any OIG policy and IT/IS protections.
- d. Open e-mails or other messages from suspicious sources (e.g., sources that you do not recognize as legitimate).
- e. Visit untrustworthy or inappropriate Web sites. For example, I will pay careful attention to the Universal Resource Locator (URL) of a web site inasmuch as URLs for malicious or untrustworthy web sites may look identical to a legitimate web site, but the URL may use a variation in spelling or a different domain (e.g., .com instead of net; or .com in place of .gov).
- f. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).
- g. Create or intentionally spread malicious code (i.e. viruses and Trojans).
- h. Attempt to access any security audit trail information that may exist without authorization.
- i. Install or connect non-OIG owned or leased (including privately owned) software or hardware (e.g., PEDS, such as Palm Pilots, Blackberrys, MP3 Players...etc.) and removable media (e.g., thumb drives, memory sticks...etc.) to OIG IT/IS.
- j. Introduce wireless devices into OIG space without authorization from the OIG IT Specialist.

4. Participate in prohibited activities, including but not limited to:

- a. Download, view, or send pornography or obscene material.
 - b. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.
 - c. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional according to OIG standards of professional behavior.
 - d. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.
-

- e. Use internet "chat" services (e.g., AOL, Instant Messenger (IM), Microsoft Network IM, Yahoo IM...etc).
- f. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
- g. "Surf" through OIG files containing personal information merely for personal curiosity.
- h. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.)

Confidentiality

All material, records, data, and information which may become available to Contractor in carrying out this Agreement are confidential and must be protected from disclosure. Contractor acknowledges a duty to protect all such material, records, data, and information and understands that unauthorized disclosure of confidential records or information may constitute a misdemeanor punishable, pursuant to La. R.S. 33:9614, by a fine of not more than two thousand dollars or imprisonment for not more than one year, or both. In addition, all proprietary information relating to the OIG or IPM computer networks, including but not limited to security access codes and security features, are confidential and Contractor must protect such information from disclosure.

Acknowledgment

I acknowledge that I have read and understand the above listed Rules of Behavior. I also state that I will adhere to these Rules of Behavior and that failure to do so may constitute a security violation resulting in denial of access to OIG IT/IS networks or facilities. I also understand that violation of these rules of behavior will be reported to the appropriate authorities and may result in administrative, criminal, or other adverse disciplinary action deemed appropriate.

Printed Name: DARREN GOODRIDGE Date: 9/15/15

Employee Signature:  Last Four of SSN: xxx-xx-7665



Ultimate Technical Solutions, Inc.

Ultimate Technical Solutions, Inc. Personnel Profile

Shaun Covey
Desktop Engineer
scc@utsi.us

EXPERIENCE

Desktop Engineer

October 2013 - Present

Ultimate Technical Solutions, LLC Harvey, Louisiana

- Help desk and field support
- Troubleshooting operating system, hardware and network issues including network devices (printers, routers, switches and network attached storage devices)
- Troubleshooting and maintaining access control devices along with video surveillance equipment.

Advanced Repair Agent (ARA) Geek Squad, Best Buy

May 2012 – October
2013

Geek Squad, Metairie, Louisiana

- Lead Tech, in charge of all repairs done in store
- In charge of the supervision and training of three ARA's
- Communicating with clients about repairs done, repair status and troubleshooting problems Repair, upgrade, setup and maintain desktop and notebook computers spanning multiple operating system platforms.

Counter Intelligence Agent (CIA) Geek Squad, Best Buy

October 2007- May 2012

Barrister Global Service Network, Metairie, Louisiana

- Check in Agent, interacting with clients, providing demonstrations of product, managing setups of new computers and working with a team
- Meeting revenue and sales goals Guided co-workers with PC troubleshooting.



Ultimate Technical Solutions, Inc.

Ultimate Technical Solutions, Inc. Personnel Profile

Scot Guelfo
Desktop Engineer
sjg@utsi.us

Experience

- Desktop Engineer** 2010 - Present
Ultimate Technical Solutions, Inc. Harvey, Louisiana
- Provide IT Support to all clients while working towards the best possible solution.
 - Monitors the entire Network of numerous companies, attending to any issues that arise.
 - Occasionally provide on-site IT support ranging from malicious infections to servers not responding.
- Geek Squad Senior** 2005 - 2010
Geek Squad Metairie, Louisiana
- Manage a team of 12 PC technicians.
 - Provide on-site training and consultations.
 - Repair, upgrade, setup and maintain desktop and notebook computers spanning multiple operating system platforms.
 - Optimize budgets, publish schedule and zone map for the department on a weekly, monthly and quarterly basis.
 - Assist customers with complex situations as well as complaints, finding the best possible solution for both parties.
- Help Desk Technician** 2005
Barrister Global Service Network Metairie, Louisiana
- Provided IT Phone support.
 - Guided co-workers with PC troubleshooting.
 - Coordinated with on-site techs to enhance customer service.

Education

- Associate of Science in Information Technology-Computer Networking Systems** 2005
*ITT Technical Institute
St. Rose, Louisiana*
- High School Graduate** 2003
*Destrehan High School
Destrehan, Louisiana*

Certifications

- Certification : Microsoft Certified Technology Specialist (MCTS)
Certification : Microsoft : Microsoft Certified Professional (MCP)
Certification : Comptia : A+

Affiliations & Organizations

Servron, LLC



Ultimate Technical Solutions, Inc.

Ultimate Technical Solutions, Inc. Personnel Profile

Edward R. Gabriel III
Network Operating Center Manager
erg@utsi.us

EXPERIENCE

Network Operating Center Manger / Senior Engineer

Jan 2006 - Present

Ultimate Technical Solutions Harvey, LA

- Supervise technical staff, providing technical guidance and direction, and manage staff development, training and performance.
- Manage customer relationships and technical services in various fields including public, private and educational sectors.
- Manage in-house desktop/system engineers, outsourced technical positions and engineers on various size projects.
- Responsible for establishing, building and maintaining new relationships with customers and vendors.
- Network Operations Service Technician, Desktop And Server deployments, Service Calls
- Server upgrades, Help Desk Administrator, Data Migration, Computer Repair
- Warehouse Management, Shipping and Receiving. etc.

Desktop Technician

Jan 2002 – Oct 2005

Dolphin Technologies New Orleans, LA

- Hardware & software integration
- Network integration
- Maintenance help desk support, Emergency response

Support Technician II

Mar 2005 - Aug 2005

Harrah's Casino & Hotel New Orleans New Orleans, LA

- Support Technician Responsible for running hourly checks on game net unix system, moving and installing of telephone lines on Avea PBX phone and voice mail system, setup A/V Equipment for meetings and pretensions.
- Answer help desk phone and solve problems, support office computers and printers
- Troubleshoot and Maintaining P.O.S (point of sale) micros terminals, Running end of day backups and end of day Procedures.

Helpdesk Technician

Apr 2004 - Mar 2005

U.S. Postal Service New Orleans, LA

- Help desk Support Technician responsible for two area codes
- post-office computer systems, networks, wireless networks and network printers, telephones, BlackBerry's, Pda's, including peripherals

Computer Technician/Help Desk

Jun 2003 - Jan 2004

Bellwether Technology. Corp New Orleans, LA

- Help desk Technician, Working at ConocoPhillips Oil Refinery
- Assisted with computer Implantation /imaging from Windows 2000 to XP Gained excellent

experience in System operations and various types of hardware and software. Gained experience dealing with the Individual concerns.

Instructor

Jun 2002 - Aug 2002

Dell TechKnow New Orleans, LA

- Provided its K-12 customers a turnkey educational approach to bridging the digital divides.
- TechKnow students gain relevant and highly marketable 21st Century skills regarded across industries and professions as necessities for effective contribution to the global workforce –such as, creative and critical thinking, problem solving, effective communication and collaboration, technology operation and concepts.

Instructor

May 1999 - Jul 2002

New Orleans Science & Math High School New Orleans, LA

- Gained knowledge in the setup of networking, computers, install cabling, servicing and repairing donated computers, troubleshooting problems.

EDUCATION

Computer Information Technology

2007

New Horizons
Metairie, LA

Computer Information Technology

2003

Delgado
Metairie, LA

High School Graduate – Computer Information Systems

2002

New Orleans Science & Math High School
New Orleans, LA

AWARDS & RECOGNITIONS

- Microsoft® Certified Systems Professional (MCP)
- Microsoft® Certified Technology Specialist (MCTS)
- MCTS: Windows® 7, Configuration (MCTS)
- CompTIA A+ certification (A+)
- Lenovo Warranty & Repair Certification



Ultimate Technical Solutions, Inc.

Ultimate Technical Solutions, Inc. Personnel Profile

Darren Goodridge

Project Manager / VCIO

dbg@utsi.us

EXPERIENCE

Project Manager / VCIO

2012 - Present

Ultimate Technical Solutions Harvey, LA

- Senior Engineer on Helpdesk and support teams.
- Work on Help Desk tickets that come in via phone or email
- Technical support at the network level: WAN and LAN connectivity, routers, firewalls, and security
- Microsoft AD Domain Environment Support
- Linux systems installations and design.
- 3rd line Support for issues involving Microsoft's core business applications and operating systems
- Was responsible for managing and coordinating the NOC team.
- Managed systems with users, customers, vendors, engineers and the whole technical team.
- Ensured that the customer \ client systems and technology used are constantly upgraded and remain relevant.
- Worked with customers and clients with solutions to fix various networking\system problems and ensured that customer needs are properly defined and satisfactorily met.
- Was responsible for informing Management, partners and peers about network/systems performance and service availability.
- Provide planning, budgeting, and strategic direction to our clients.
- Manage new client on-boarding process.
- Act as the main point of contact both to the client and our organization.
- Developed assessments of the current environment, and strategic technology plan and budget for each client
- Deliver monthly and quarterly reports for clients for there support in regards to services provided and IT infrastructure health.
- Manging Projects for clients from small systems installs to large migration projects
- Provide a monthly systems review with clients in regards to IT plan and budget progress and their satisfaction with UTSI support.
- Maintain communication with the NOC Manager and Helpdesk staff to make them aware of issues and trends in regards to client Support.
- Maintain communications with the UTSI NOC Manager to be aware of issues with consulting project issues and completion times to keep support at top level.

IT Director

2007 – 2012

RS Hall Engineering, Thirsk, United Kingdom

- Elevated this company from one PC with SAGE payroll and Windows XP to a complete server workstation environment, which included 8 servers, 250 workstations over 4 satellite offices.
- Created a program which included sage manufacturing, sage line 50 and payroll to enable this

company to manage and control all aspects of its manufacturing.

- Created a program allowing the importing/exporting of Navision and QuickBooks financial reports with Sage.
- Resolved production issues with plant floor by performing root-cause analysis of work flow issues using techniques that included document traffic flow and quality assurance.
- Implemented a sales program for customer service staff members including a full email and website ordering system allowing staff to receive customer orders via email fax or phone to input into the system.
- Created and implemented a new computerized stock control system.
- Participated in executive staff meetings involving the management of the company.
- Managed four different locations with a staff of six
- Implemented a total new VOIP system
- Increased production by 34% and company value by 200% with the implementation of new work systems and programs.
- Responsible for maintaining budgets for multiple sites and corporate IT department, including specific project budgets
- Liaised with outside technology suppliers for latest technology.

Senior Support Engineer

2005 - 2007

ADA Computer Systems, Burgess Hill, United Kingdom

- Senior Engineer on Helpdesk and support teams.
- Day to day customer support and managing engineers.
- Implemented a new system to streamline customer inquiries and problems by using Navision 3, improving customer support turnaround time by 38%.
- Responsible for internal ISP support, including customer websites and hosting.
- Implemented Good Technology smart phones, and subsequently transferred company to Blackberry systems
- Performed site visits and provided customer service to install and service Good Technology and Blackberry servers and phones.

Support Engineer

2000 - 2005

Pinnacle Internet Services, Worthing, United Kingdom

- 1st/2nd line support role
- Managed company's ADSL and SDSL systems.
- Managed companies email, web and hosting servers.
- Wrote CAST program, a web content management system allowing the editing and construction of business based websites.
- CAST program was wholly adopted by Pinnacle and was a major factor in the decision to purchase Pinnacle by Precedent communications

EDUCATION

University of Hertfordshire

*Bachelors of Arts in Computer Science and Business Information
Technology
United Kingdom*

TRAINING

Microsoft Training Academy

- Microsoft Certified Professional Windows NT 3.51, XP, Vista and 7 Inc. TCP-IP, BIND, DNS and AD Design and Security
- Microsoft Certified Professional Server NT, 2003, 2008 (R2) Server 2012 R2 & SQL Server 2005 and 2008.
- Microsoft Certified Systems Engineer –Windows Server and Exchange

AWARDS & RECOGNITIONS

- HP Certified Systems Engineer
- Microsoft Certified Systems Engineer

Ultimate Technical Solutions, Inc.