

**Department of Corrections  
Memorandum of Understanding  
Contract Number DOC-14-074**

The Virginia Department of Corrections (“DOC”) and JPay, Inc. (“Contractor”) have agreed to the following:

**A. GENERAL:**

1. The purpose of this Contract for JP3 and or JP4 players is to allow the Commonwealth of Virginia Department of Corrections offenders at Security Levels 1, 2, 3, 4, 5 and Red Onion State prison the opportunity to purchase music, and non-music (word) audio files for fiction, non-fiction, poetry, etc. in an “MP3” mode and to purchase JP3 and or JP4 players. See Attachment A and B for the current approved music catalog and the current approved list of religious material which may be purchased by offenders. This Contract will also include an offender email pilot offered at sites with kiosks at prisons designated by the DOC. DOC will execute an initial one year contract, with four, one-year optional renewal periods.
2. The DOC is organized into three regions: Western, Central and Eastern. Correctional facilities that are currently utilizing this service are: Red Onion State Prison, Wallens Ridge State Prison, Sussex I State Prison, Sussex II State Prisons, Keen Mountain Correctional Center and Nottoway Correctional Center. Attachment E lists each correctional facility and the region in which the current facilities are located. This contract will allow for the expansion of these services to additional DOC facilities at an estimated rate of 10-12 facilities per quarter, beginning in December, 2013. Additional information about the Commonwealth of Virginia, Department of Corrections is available on the DOC website at [www.vadoc.virginia.gov](http://www.vadoc.virginia.gov).

**B. SECURITY REQUIREMENTS:**

1. The Contractor shall adhere to all DOC security requirements. See Attachment F “Security Requirements” for list of standard facility security requirements.
2. The Contractor and all software, systems, or personnel who will use or access the DOC’s systems shall adhere to all applicable Virginia Information Technologies Agency and the DOC IT Security policies and procedures. See Attachment G “Information Technology Security”.

**C. CONTRACTOR RESPONSIBILITIES:**

1. The Contractor shall administer all aspects of the sales operation, including but not limited to: selling the MP3 player directly to the offender and providing the device to access/download the audio files. All audio files offered to the offenders for sale shall be the industry “sanitized” versions. The Contractor shall provide staff to download music in those facilities where offenders do not have access to the device.
2. In addition, the Contractor shall provide an appropriate number of catalogues and order forms to participating facilities (either in paper or electronic format), process the orders and

- schedule the individual offenders to access/receive their orders. The catalog does not have to list every audio selection available, but should outline the genres offered.
3. The Contractor shall provide this service at no cost to the DOC. All charges for the JP3 and or JP4 players and the audio download shall be paid by the offenders based on negotiated rates.
  4. The Contractor shall make available all audio files except those from the DOC list of disapproved publications and disapproved music (See Attachments C and D). The DOC will be given the opportunity to request product samples on a no-charge basis for screening of the product content by the DOC Publications Review or Music Review Committee.
  5. The Contractor shall distribute a catalog tailored to the DOC on an annual basis. The Contractor is responsible for ensuring that the publications listed on the DOC disapproved Publications, and disapproved Music lists are NOT available for sale to DOC offenders. The DOC reserves the right to revise the list as necessary. Changes to the catalog including but not limited to the addition or deletion of publications may be issued via a catalog supplement.
  6. The Contractor shall provide the media catalog electronically on the kiosks.
  7. All order fees are the responsibility of the offender. Payment from the offender to the Contractor may be handled through Kiosks whereby the offenders will be able to purchase either media credits or song titles on the kiosks using funds from their commissary accounts. Friends and family members will also be able to purchase JPay Credits and purchase a JPay Media Player on behalf of an offender from JPay.com. The DOC shall not be held liable for payment of the goods ordered. Should a mistake be made the Contractor shall contact the Business Manager at the respective DOC facility for resolution.
  8. Each order shall be electronically transferred (downloaded) individually at a kiosk or other distribution device. An individual invoice shall be marked paid and electronically emailed to the offender or the friend and family member or posted to the "my player" section of the offender's kiosk login page upon request. The invoice shall include: offender name, offender ID number, housing pod/cell block and facility name and address.
  9. All downloads shall be processed by the Contractor and delivered to the offender within 5 to 7 working days after the Contractor's receipt of the Offender Order Form which will also indicate offender payment verification.
  10. At the time of delivery, if an offender is not at the facility where the original order was placed, the facility will notify the Contractor of the actual location of the offender. If the offender has been transferred to one of the listed pilot facilities, it is the Contractor's responsibility to promptly deliver the download to the proper facility at the Contractor's expense. If the offender has been transferred to a facility that is not participating in the pilot, the Contractor shall ensure that the offender's device will function independently of the kiosks at whichever prison the offender transfers to. In the event the offender is transferred to a facility which does not have the JP3 and or JP4 player program, the JP3 and or JP4 player will be stored in the facility's personal property area and held for the offender until the offender is again transferred and discharged, or the JP3 and or JP4 program is expanded to that facility.

11. The Contractor shall resolve any quality problems, discrepancies, duplicate shipments, damaged items, or other problems within twenty one working days, without assessing re-stocking charges.
12. The Contractor shall maintain sufficient inventory to meet offender purchase requirements. The Contractor shall be able to meet a 95 % or better fill rate on all orders of JP3 and or JP4 players and the audio files. The Contractor shall include all charges to include the unit cost of each audio file, shipping and handling, and applicable state sales tax in the total unit pricing. Back-orders will be filled within thirty days after receipt of the order. If it is still on back-order after thirty days, the order shall be cancelled and payment refunded. The DOC will allow offenders to submit special requests for materials that are not listed in the approved catalog, however, before the special orders are processed, the DOC must review and approve the content of the special order.
13. New word audio files may be added by the Contractor and included in the DOC catalog only after review and approval by the DOC Publications Review Committee. The Contractor shall furnish samples of audio files at no charge to the DOC. The DOC Publications Review Committee will require a minimum of thirty days after receipt of sample(s) for review and response.
14. New music files may be added as long as they do not possess a "Parental Advisory" notice on them.
15. The Contractor shall not sell uncut versions, or products recorded in languages other than English or Spanish.
16. The Contractor shall not offer for sale to DOC offenders demos or pirated product material.
17. No formats other than JP3 and or JP4 will be allowed for sale to DOC offenders. No additional item or items can be included in the audio files including DVD's and/or burned CDs.
18. The Contractor must be capable of providing a complete order history of all transactions for each offender. The report shall be generated upon DOC request.
19. The Contractor shall have the capability of acknowledging and tracking all orders.
20. The Contractor shall submit an activity report to the DOC quarterly and upon request. The activity report shall include by facility, total number of units ordered and total dollar amount of sales.

**D. PERSONNEL ATTENDANCE:**

In instances where personnel attendance is required at the DOC's premises to perform support services, the DOC shall not be responsible for travel costs.

**E. PRICING AND COMMISSION**

Pricing will be reasonable and conform to market value as evaluated by the DOC.

1. Commissions: Purchasing music/audio file -5% per item
2. Purchasing playing device (MP3, MP4) -\$5.00 per device.
3. Email (outbound message) - .05 ( 5 cents) per outbound message.

**F. WARRANTY:**

Any parts and labor provided relative to extended services are warranted for a period of one year. JP3 and JP4 Devices are warranted for 90 days. Damage to systems or components due to abuse, negligence or acts of God are excluded from the warranty provisions.

## ATTACHMENT I

**GENERAL TERMS AND CONDITIONS:****A. VENDORS MANUAL:**

This Contract is subject to the provisions of the Commonwealth of Virginia *Vendors Manual* and any revisions thereto, which are hereby incorporated into this contract in their entirety. The procedure for filing contractual claims is in section 7.19 of the *Vendors Manual*. A copy of the manual is normally available for review at the purchasing office and is accessible on the Internet at [www.eva.virginia.gov/learn-about-eva/vendors-manual](http://www.eva.virginia.gov/learn-about-eva/vendors-manual) under "Manuals".

**B. APPLICABLE LAWS AND COURTS:**

This Contract shall be governed in all respects by the laws of the Commonwealth of Virginia and any litigation with respect thereto shall be brought in the courts of the Commonwealth. The agency and the Contractor are encouraged to resolve any issues in controversy arising from the award of the contract or any contractual dispute using Alternative Dispute Resolution (ADR) procedures (*Code of Virginia*, §2.2-4366). ADR procedures are described in Chapter 9 of the *Vendors Manual*. The Contractor shall comply with all applicable federal, state and local laws, rules and regulations.

**C. ANTI-DISCRIMINATION:**

By entering into this Contract, the Contractor certifies to the Commonwealth that the Contractor will conform to the provisions of the Federal Civil Rights Act of 1964, as amended, as well as the Virginia Fair Employment Contracting Act of 1975, as amended, where applicable, the Virginians With Disabilities Act, the Americans With Disabilities Act and §2.2-4311 of the *Virginia Public Procurement Act*. If the Contractor is a faith-based organization, the organization shall not discriminate against any recipient of goods, services, or disbursements made pursuant to the contract on the basis of the recipient's religion, religious belief, refusal to participate in a religious practice, or on the basis of race, age, color, gender or national origin and shall be subject to the same rules as other organizations that contract with public bodies to account for the use of the funds provided; however, if the faith-based organization segregates public funds into separate accounts, only the accounts and programs funded with public funds shall be subject to audit by the public body. (*Code of Virginia*, §2.2-4343.1E)

In every contract over \$10,000 the provisions in 1. and 2. below apply:

1. During the performance of this contract, the Contractor agrees as follows:
  - a. The Contractor will not discriminate against any employee or applicant for employment because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment, except where there is a bona fide occupational qualification reasonably necessary to the normal operation of the Contractor. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

- b. The Contractor, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, will state that such Contractor is an equal opportunity employer.
  - c. Notices, advertisements and solicitations placed in accordance with federal law, rule or regulation shall be deemed sufficient for the purpose of meeting these requirements.
2. The Contractor will include the provisions of 1. above in every subcontract or purchase order over \$10,000, so that the provisions will be binding upon each subcontractor or vendor.

**D. ETHICS IN PUBLIC CONTRACTING:**

By entering into this Contract, the Contractor certifies that this Contract is entered into without collusion or fraud and that the Contractor has not offered or received any kickbacks or inducements from any other supplier, manufacturer or subcontractor in connection with this Contract, and that the Contractor has not conferred on any public employee having official responsibility for this procurement transaction any payment, loan, subscription, advance, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.

**E. IMMIGRATION REFORM AND CONTROL ACT OF 1986:**

By entering into a written contract with the Commonwealth of Virginia, the Contractor certifies that the Contractor does not, and shall not during the performance of the contract for goods and services in the Commonwealth, knowingly employ an unauthorized alien as defined in the federal Immigration Reform and Control Act of 1986.

**F. DEBARMENT STATUS:**

By entering into this contract, the Contractor certifies that the Contractor is not currently debarred by the Commonwealth of Virginia from submitting bids or bids on contracts for the type of goods and/or services covered by this Contract, nor is the Contractor an agent of any person or entity that is currently so debarred.

**G. ANTITRUST:**

By entering into this contract, the Contractor conveys, sells, assigns, and transfers to the Commonwealth of Virginia all rights, title and interest in and to all causes of action it may now have or hereafter acquire under the antitrust laws of the United States and the Commonwealth of Virginia, relating to the particular goods or services purchased or acquired by the Commonwealth of Virginia under said contract.

**H. PAYMENT:**

1. To Prime Contractor:

- a. Invoices for items ordered, delivered and accepted shall be submitted by the Contractor directly to the payment address shown on the purchase order/contract. All invoices shall show the state contract number and/or purchase order number, social security number (for individual Contractors) or the federal employer identification number (for proprietorships, partnerships, and corporations).

- b. Any payment terms requiring payment in less than 30 days will be regarded as requiring payment 30 days after invoice or delivery, whichever occurs last. This shall not affect offers of discounts for payment in less than 30 days, however.
- c. All goods or services provided under this contract or any purchase order against this contract, that are to be paid for with public funds, shall be billed by the Contractor at the contract price, regardless of which public agency is being billed.
- d. The following shall be deemed to be the date of payment: the date of postmark in all cases where payment is made by mail, or the date of offset when offset proceedings have been instituted as authorized under the Virginia Debt Collection Act.
- e. **Unreasonable Charges.** Under certain emergency procurements and for most time and material purchases, final job costs cannot be accurately determined at the time orders are placed. In such cases, Contractors should be put on notice that final payment in full is contingent on a determination of reasonableness with respect to all invoiced charges. Charges, which appear to be unreasonable, will be researched and challenged, and that portion of the invoice held in abeyance until a settlement can be reached. Upon determining that invoiced charges are not reasonable, the Commonwealth shall promptly notify the Contractor, in writing, as to those charges, which it considers unreasonable, and the basis for the determination. A Contractor may not institute legal action unless a settlement cannot be reached within thirty (30) days of notification. The provisions of this section do not relieve an agency of its prompt payment obligations with respect to those charges, which are not in dispute (*Code of Virginia*, §2.2-4363).

2. To Subcontractors:

- a. The Contractor is hereby obligated:
  - (1). To pay the subcontractor(s) within seven (7) days of the Contractor's receipt of payment from the Commonwealth for the proportionate share of the payment received for work performed by the subcontractor(s) under the contract; or
  - (2). To notify the agency and the subcontractor(s), in writing, of the Contractor's intention to withhold payment and the reason.
- b. The Contractor is obligated to pay the subcontractor(s) interest at the rate of one percent per month (unless otherwise provided under the terms of the contract) on all amounts owed by the Contractor that remain unpaid seven (7) days following receipt of payment from the Commonwealth, except for amounts withheld as stated in (2) above. The date of mailing of any payment by U. S. Mail is deemed to be payment to the addressee. These provisions apply to each sub-tier Contractor performing under the primary contract. A Contractor's obligation to pay an interest charge to a

subcontractor may not be construed to be an obligation of the Commonwealth.

3. Each prime Contractor who enters into a contract in which provision of a SWaM procurement plan is a condition to the award, shall deliver to the contracting agency or institution, on or before request for final payment, evidence and certification of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the SWaM procurement plan. Final payment under the contract in question may be withheld until such certification is delivered and, if necessary, confirmed by the agency or institution, or other appropriate penalties may be assessed in lieu of withholding such payment.
4. The Commonwealth of Virginia encourages contractors and subcontractors to accept electronic and credit card payments.

**I. PRECEDENCE OF TERMS:**

The following General Terms and Conditions: VENDORS MANUAL, APPLICABLE LAWS AND COURTS, ANTI-DISCRIMINATION, ETHICS IN PUBLIC CONTRACTING, IMMIGRATION REFORM AND CONTROL ACT OF 1986, DEBARMENT STATUS, ANTITRUST, MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS, CLARIFICATION OF TERMS, PAYMENT shall apply in all instances. In the event there is a conflict between any of the other General Terms and Conditions and any Special Terms and Conditions in this Contract, the Special Terms and Conditions shall apply.

**J. CHANGES TO THE CONTRACT:**

Changes can be made to the contract in any of the following ways:

1. The parties may agree in writing to modify the scope of the contract. An increase or decrease in the price of the contract resulting from such modification shall be agreed to by the parties as a part of their written agreement to modify the scope of the contract.
2. The Department of Corrections may order changes within the general scope of the contract at any time by written notice to the Contractor. Changes within the scope of the contract include, but are not limited to, things such as services to be performed, the method of packing or shipment, and the place of delivery or installation. The Contractor shall comply with the notice upon receipt. The Contractor shall be compensated for any additional costs incurred as the result of such order and shall give the Department of Corrections a credit for any savings. Said compensation shall be determined by one of the following methods:
  - a. By mutual agreement between the parties in writing; or
  - b. By agreeing upon a unit price or using a unit price set forth in the contract, if the work to be done can be expressed in units, and the Contractor accounts for the number of units of work performed, subject to the Department of Correction's right to audit the Contractor's records and/or to determine the correct number of units independently; or



- c. By ordering the Contractor to proceed with the work and keep a record of all costs incurred and savings realized. A markup for overhead and profit may be allowed if provided by the contract. The same markup shall be used for determining a decrease in price as the result of savings realized. The Contractor shall present the Department of Corrections with all vouchers and records of expenses incurred and savings realized. The Department of Corrections shall have the right to audit the records of the Contractor, as it deems necessary to determine costs or savings. Any claim for an adjustment in price under this provision must be asserted by written notice to the Department of Corrections within thirty (30) days from the date of receipt of the written order from the Department of Corrections. If the parties fail to agree on an amount of adjustment, the question of an increase or decrease in the contract price or time for performance shall be resolved in accordance with the procedures for resolving disputes provided by the Disputes Clause of this contract or, if there is none, in accordance with the disputes provisions of the Commonwealth of Virginia *Vendors Manual*. Neither the existence of a claim nor a dispute resolution process, litigation or any other provision of this contract shall excuse the Contractor from promptly complying with the changes ordered by the Department of Corrections or with the performance of the contract generally.

**K. INSURANCE:**

By entering into this Contract, the Contractor certifies that it has the following insurance coverage. The Contractor further certifies that the Contractor and any subcontractors will maintain this insurance coverage during the entire term of the contract and that all insurance coverage will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

The Contractor shall provide a current Certificate of Insurance naming the Commonwealth of Virginia, Department of Corrections as an additional insured for the stipulated coverage and shall include the applicable contract number and Contractor's name on the certificate.

**INSURANCE COVERAGES AND LIMITS REQUIRED:**

1. Worker's Compensation – Statutory requirements and benefits. Coverage is compulsory for employers of three or more employees, to include the employer. Contractors who fail to notify the Commonwealth of increases in the number of employees that change their workers' compensation under the *Code of Virginia* during the course of the contract shall be in noncompliance with the contract.
2. Employers Liability - \$100,000.
3. Commercial General Liability - \$1,000,000 per occurrence. Commercial General Liability is to include bodily injury and property damage, personal injury and advertising injury, products and completed operations coverage. The Commonwealth of Virginia must be named as an additional insured and so endorsed on the policy.

**L. DRUG FREE WORKPLACE:**

During the performance of this contract, the Contractor agrees to (i) provide a drug-free workplace for the Contractor's employees, (ii) post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance, marijuana or alcohol is prohibited in the Contractor's workplace and specifying the actions that will be taken against employees for violations of such prohibition; (iii) state in all solicitations or advertisements for employees placed by or on behalf of the Contractor that the Contractor maintains a drug-free workplace; and (iv) include the provisions of the foregoing clauses in every subcontract or purchase order of over \$10,000, so that the provisions will be binding upon each subcontractor or vendor.

For the purposes of this section, "drug-free workplace" means a site for the performance of work done in connection with a specific contract awarded to a Contractor in accordance with this chapter, the employees of whom are prohibited from engaging in the unlawful manufacture, sale, distribution, dispensation, possession or use of any controlled substance, marijuana or alcohol during the performance of the contract.

**M. NONDISCRIMINATION OF CONTRACTORS:**

If the Contractor is a faith-based organization and an individual, who applies for or receives goods, services, or disbursements provided pursuant to this contract objects to the religious character of the faith-based organization from which the individual receives or would receive the goods, services, or disbursements, the public body shall offer the individual, within a reasonable period of time after the date of his objection, access to equivalent goods, services, or disbursements from an alternative provider.

**N. AUTHORIZATION TO CONDUCT BUSINESS IN THE COMMONWEALTH:**

A contractor organized as a stock or nonstock corporation, limited liability company, business trust, or limited partnership or registered as a registered limited liability partnership shall be authorized to transact business in the Commonwealth as a domestic or foreign business entity if so required by Title 13.1 or Title 50 of the *Code of Virginia* or as otherwise required by law. Any business entity described above that enters into a contract with a public body pursuant to the *Virginia Public Procurement Act* shall not allow its existence to lapse or its certificate of authority or registration to transact business in the Commonwealth, if so required under Title 13.1 or Title 50, to be revoked or cancelled at any time during the term of the contract. A public body may void any contract with a business entity if the business entity fails to remain in compliance with the provisions of this section

**ATTACHMENT II****SPECIAL TERMS AND CONDITIONS:****A. AUDIT:**

The Contractor shall retain all books, records, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. The agency, its authorized agents, and/or state auditors shall have full access to and the right to examine any of said materials during said period.

**B. CANCELLATION OF CONTRACT:**

The Purchasing Agency reserves the right to cancel and terminate any contract, in part or in whole, without penalty, upon 60 days written notice to the Contractor. In the event the initial contract period is for more than 12 months, the contract may be terminated by either party, without penalty, after the initial 12 months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

**C. CONFIDENTIAL INFORMATION:**

The Contractor acknowledges that in the performance of this contract, confidential and proprietary offender information will be made available to the Contractor. The Contractor agrees to maintain the confidentiality of the offender information. The Contractor will not disclose any offender information to any third party without prior written authorization from the DOC. These obligations will apply to verbal information as well as specific portions of information that are disclosed in writing or other tangible form.

**D. HIRING PRACTICES:**

In the event a Contractor proposes to employ ex-offenders, the DOC may determine that it is not in the best interest to allow some ex-offenders to provide service. Some of the factors that the DOC may consider are: where the ex-offender served time, the nature of the crime and the length of time since sentence obligation was completed.

**E. INDEMNIFICATION:**

Contractor agrees to indemnify, defend and hold harmless the Commonwealth of Virginia, its officers, agents, and employees from any claims, damages and actions of any kind or nature, whether , at law or in equity, arising from or caused by the use of any materials, goods, or equipment of any kind or nature furnished by the Contractor/any services of any kind or nature furnished by the Contractor, provided that such liability is not attributable to the sole negligence of the using agency or to failure of the using agency to use the materials, goods, or equipment in the manner already and permanently described by the Contractor on the materials, goods or equipment delivered.

**F. PRIME CONTRACTOR RESPONSIBILITIES:**

The Contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors, that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the prime Contractor. The Contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

**G. SUBCONTRACTS:**

No portion of the work shall be subcontracted without prior written consent of the Purchasing Agency. In the event that the Contractor desires to subcontract some part of the work specified herein, the Contractor shall furnish the Purchasing Agency the names, qualifications and experience of their proposed subcontractors. The Contractor shall, however, remain fully liable and responsible for the work to be done by its subcontractor(s) and shall assure compliance with all requirements of the contract.

**H. BACKGROUND CHECKS:**

As defined in DOC Procedure 030.3, the DOC may require partial or limited background investigations for Contractor staff assigned to this Contract. The Contractor shall be required to pay for all background investigations processed for staff. Investigations are charged at a rate of \$90.00 for a partial background check and \$50.00 for a limited background check. Fees are on a per-investigation basis and will be invoiced by DOC Account Receivable. Contractor employees will be required to complete the Authority for Release of Information (Form 030\_F0\_3-11). The Contractor shall allow the DOC Background Investigation Unit access to review the Contractor staff personnel and employment records.

If derogatory information is discovered during the background investigation(s), the DOC may require reassignment of Contractor staff or immediate cancellation of the Contract.

The DOC may, on an ongoing basis, require an updated VCIN report/background review at any time. Information obtained from this investigation may result in Contractor staff's immediate removal from state property.

The Contractor shall notify DOC Contract Administrator within 48 hours of occurrence in the event any Contractor staff assigned to provide services to the DOC is:

- charged with a criminal offense either on or off the job;
- convicted of a criminal offense of any kind; or
  - in receipt of an administrative suspension, censure or failure to renew any license, certification or professional member that is required under the terms of this contract.

Contract award may be contingent upon the Contractor and/or Contractor staff receiving a favorable report.

**I. DEFINITION - SOFTWARE:**

As used herein, the terms software, product, or software products shall include all related materials and documentation whether in machine readable or printed form.

**J. LATEST SOFTWARE VERSION:**

Any software product(s) provided under the contract shall be the latest version available to the general public as of the commencement of this contract.

**K. PRODUCT SUBSTITUTION:**

During the term of the contract, the Contractor is not authorized to substitute any item for that product and/or software identified in the contract without the prior written consent of the contracting officer or designee.

**L. QUALIFIED REPAIR PERSONNEL:**

All warranty or maintenance services to be performed on the items specified in this contract as well as any associated hardware or software shall be performed by qualified technicians properly authorized by the manufacturer to perform such services. The Commonwealth reserves the right to require proof of certification at any time during the term of the contract.

**M. SERVICE PERIOD (ROUTINE):**

Contractor shall be available during the normal working hours of 8 A.M. to 5 P.M. EST, Monday through Friday. -Please see the attached Service Level Agreement (SLA) (Attachment H) regarding repairs or corrections to the kiosks and network. Offenders are capable of repairing various software issues by plugging into the kiosks and pressing the "repair my player" feature. For all other player issues the offender will be given an RMA and can expect a new player within 30 days if the player is within warranty. If the player is not within warranty JPay will sell the offender a new one and deliver it within 30 days.

**N. SERVICES REPORTS:**

Upon completion of any maintenance call, the contractor shall provide the agency with a signed service report that includes, at a minimum: a general statement as to the problem, action taken, any materials or parts furnished or used, and the number of hours required to complete the repairs.

**O. SOFTWARE UPGRADES:**

The Commonwealth shall be entitled to any and all upgraded versions of the software covered in the contract that becomes available from the contractor. The maximum charge for upgrade shall not exceed the total difference between the cost of the Commonwealth's current version and the price the contractor sells or licenses the upgraded software under similar circumstances.

**P. TITLE TO SOFTWARE:**

The contractor represents and warrants that it is the sole owner of the software or, if not the owner, that it has received all legally required authorizations from the owner to license the software, has the full power to grant the rights required by this contract, and that neither the software nor its use in accordance with the contract will violate or infringe upon any patent, copyright, trade secret, or any other property rights of another person or organization.

**Q. WARRANTY AGAINST SHUTDOWN DEVICES:**

The contractor warrants that the equipment and software provided under the contract shall not contain any lock, counter, CPU reference, virus, worm, or other device capable of halting operations or erasing or altering data or programs. Contractor further warrants that neither it, nor its agents, employees, or subcontractors shall insert any shutdown device following delivery of the equipment and software.

**R. RENEWAL OF CONTRACT:**

This contract may be renewed by the Commonwealth upon written agreement of both parties for four optional successive one year periods, under the terms of the current contract.

**S. PRISON RAPE ELIMINATION ACT (PREA):**

Contractors and Contractors' staff, who are providing services to the Virginia Department of Corrections, and who have any level of interaction or potential for interaction with inmates shall review the Prison Rape Elimination Act (PREA) <http://www.vadoc.virginia.gov/procure/>. Contractors and Contractors' staff must receive training (at the Agency location where services are to be performed) on their responsibilities, under PREA including the Agency's sexual abuse and sexual harassment prevention, detection and response policies and procedures (including reporting). Contractors and Contractors' staff agree to abide by the Agency's zero-tolerance policy regarding fraternization, sexual abuse and sexual harassment and the obligation to report incidents.

ATTACHMENT A

APPROVED RELIGIOUS AUDIO MATERIAL

**BUDDHISM**

Naparstek Belleruth	Ease Grief #1 & #2	JEMO124B	\$22.98
One Spirit & Diarma Moon	At Ease 2*	JEMO120B	\$15.98
Sounds True	Buddhist Meditations for Beginners	JEMO122B	\$31.98
Sounds True	Insight Meditation	JEMO126B	\$137.98

**CHRISTIAN**

American Bible Society	all titles	to be provided	vary
Don Piper	90 Minutes in Heaven	JEMO128C	\$19.98

**CHRISTIAN-PROTESTANT**

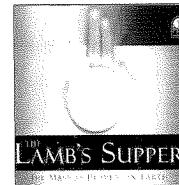
Adventures in Odyssey Focus on the Family	all titles	to be provided	vary
Alistair Begg	Truth Partner (various titles)	to be provided	vary
Andre and Linda	Altar Call	JEMO136CP	\$15.98
Andrew Womack Ministries	all titles	to be provided	vary
Anne Graham Lotz	all titles	to be provided	vary
Anne Lamott	Grace Eventually: Thoughts on Faith	JEMO148CP	\$28.98
Art Mathias	Biblical Foundations (series)	JEMO138CP	\$50.98
			to \$75.98
Benny Hinn Ministries	all titles	to be provided	vary
Berean Baptist Church	all titles	to be provided	\$10.98
Beth Moore	all titles	to be provided	vary
Bill Hybels	all titles	to be provided	vary
Bill Winston	Renewing the Mind	JEMO174CP	\$14.98
Billy Brim	all titles	to be provided	vary
Billy Graham/Evangelistic Association	all titles	to be provided	vary
Bishop Eddie Long	all titles	to be provided	vary
Bishop Paul S. Morton	all titles	to be provided	vary
Brian Doerksen	Today	JEMO182CP	\$14.98
C.S. Lewis (author)	all titles	to be provided	vary
Charles (Chuck) Swindoll	all titles	to be provided	vary
Charles Stanley/In Touch Ministries	all titles	to be provided	vary
Chip Ingram	Living on the Edge	JEMO162CP	\$35.98
Chris Gardner	Pursuit of Happiness	JEMO172CP	\$34.98
Christian Instruction Zondervan	Boundaries	JEMO140CP	\$28.98
Cynthia Hale	all titles	to be provided	vary
Dave Hunt	In Christ Jesus	JEMO158CP	\$20.98
David Hocking/James Durbin Communications	Hope for Today	JEMO154CP	\$10.98
David Wilkerson Times Square Church	all titles	to be provided	vary
Dee Henderson	Truth Seeker*	JEMO188CP	\$99.98
Dr. Creffo Dollar	all titles	to be provided	vary
Dr. David Jeremiah	all titles	to be provided	vary
Dr. Joel Gregory	all titles	to be provided	vary
Dr. Oliver Greene/The Gospel Hour Program	all titles	to be provided	vary
Duplantis Ministries	How to Get From Believing to Knowing	JEMO156CP	\$12.98
Dwight Fryor	all titles	to be provided	vary
E.M. Bounds	all titles	to be provided	vary
Ed Dobson	Prayers & Promises When Facing Illnesses	JEMO168CP	\$24.98
Eddie Long	all titles	to be provided	vary
Ever Increasing Faith Ministries	all titles	to be provided	vary
Focus on the Family/James Dobson	all titles	to be provided	vary
Gloria Copeland (Kenneth Copeland Ministries)	all titles	to be provided	vary
Good News Broadcasting Association	all titles	to be provided	vary
Graham Cooke	all titles	to be provided	vary
Henry and Richard Blackaby	Hearing God's Voice	JEMO150CP	\$21.98
Hope Aglow Ministries	all titles	to be provided	vary
Jamal Bryant	all titles	to be provided	vary
Jesse Duplantis	all titles	to be provided	vary
Jim Cymbala	Fresh Power*	JEMO146CP	\$60.98

\*May only be available in used condition.

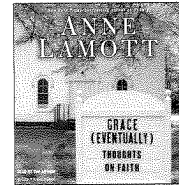
Joe Crews	all titles	to be provided	vary
Joel Osteen	all titles	to be provided	vary
John Bevere Ministries	Drawing Near:		
	A Life of Intimacy with God (3PC)*	JEMO142CP	\$41.98
	The Pilgrim's Progress	JEMO178CP	\$31.98
John Bunyan	all titles	to be provided	\$7.98
John Clayton	all titles	to be provided	vary
John MacArthur	all titles	to be provided	vary
John R.W. Stott	all titles	to be provided	vary
Josh McDowell	all titles	to be provided	vary
Joyce Meyer Ministries	all titles	to be provided	vary
Kay Arthur	all titles	to be provided	vary
Kenneth Copeland Ministries	all titles	to be provided	vary
Kenneth Hagin Ministries	all titles	to be provided	vary
Key Life Ministries	all titles	to be provided	vary
Lee Strobel	all titles	to be provided	vary
Lisa Bevere	Purity's Power*	JEMO170CP	\$24.98
Luther Barnes	Wherever I Go	JEMO190CP	\$17.98
Lynn Hiles Ministries	all titles	to be provided	vary
Lynne Hammond	all titles	to be provided	vary
Marilyn Hickey Ministries	all titles	to be provided	vary
Max Lucado/Upward Ministries	all titles	to be provided	vary
McGee	Married Beyond Recognition	JEMO164CP	\$19.98
Michael Pearl	Righteousness*	JEMO176CP	\$15.98
Nicky Cruz	all titles	to be provided	vary
No Greater Joy Ministries	all titles	to be provided	vary
Oral Roberts Evangelistic Association	all titles	to be provided	vary
Otto Koning	The Pineapple Story Series	JEMO180CP	\$40.98
Pastor B. Courtney McBath	all titles	to be provided	vary
Pastor Chuck Smith/Daily Study	all titles	to be provided	vary
Pastor Jesse Duplantis	Nothing is Impossible	JEMO166CP	\$12.98
Pat Robertson/Christian Broadcast Network	all titles	to be provided	vary
Paula White Ministries	all titles	to be provided	vary
Perry Stone	all titles	to be provided	vary
Phil Kidd	A Glimpse of Glory	JEMO132C	\$15.98
Philip Yancey	all titles	to be provided	vary
Promise Keepers	all titles	to be provided	vary
R.T. Kendall	Total Forgiveness #1 & #2	JEMO184CP	\$20.98
Radio Bible Class	all titles	to be provided	vary
Ravi Zacharias Ministries RZIM	all titles	to be provided	vary
Ray Comfort	Hell's Best Kept Secret	JEMO152CP	\$10.98
Rick Joyner/Morning Star Publications	all titles	to be provided	vary
Rick Warren/Saddleback Community Church	all titles	to be provided	vary
Rodney Howard/Browne Ministries	all titles	to be provided	vary
Spurgeon	All of Grace	JEMO134C	\$18.98
Stephen Arterburn	Every Young Man's Battle	JEMO144CP	\$67.98



C.S. Lewis  
all titles  
to be provided \$ vary



Dr. Scott Hahn  
The Lamb's Supper  
JEMO198RC \$ 25.98



Anne Lamott  
Grace Eventually  
JEMO148CP \$ 28.98

\*May only be available in used condition.

**ATTACHMENT B**

**APPROVED MUSIC AUDIO/BOOK MATERIALS**

(See PDF electronic file ATTACHMENT B DOC-14-074 JPay)



ATTACHMENT C

DISAPPROVED MUSIC CDS

Hood Internet  
Z-Trip  
Diplo  
Steve Aoki-Wonderland  
Jay-Z “American Gangster”  
50CENT “The Massacre”  
8 Balls and MJG  
Gucci Mane “Back to the Traphouse”  
Gucci Mane “Hard to Kill”  
The Game “The Documentary”  
Based on a T.R.U. Story  
Dreams and Nightmares  
Trouble Man  
Paper Trail  
Duets  
All Eyes on Me  
Greatest Hits  
Emeritus  
Mad  
I Need Mine Flesh of My Flesh, Blood of My Blood  
Americkz NightMare  
Let’s Get It: Thugh Motivation 101  
The B Coming  
The Black Album  
The Documentary  
The Massacre  
Self Made 2  
R. Kelly TP-2.com  
Get Rich or Die Trying  
Already Platinum  
Life 268-192  
Shallow Life by Lacuna Coil  
Anthems of Rebellion by Arch Enemy  
Subliminal Verses, by Slipknot  
Insane Clown Posse (all titles)  
All CDs labeled as “Explicit Lyrics”  
Wonderland  
Notorious B.I.G. (all titles)  
Snoop Dog (all titles)  
Rare Essence (all titles)  
Gods of War by ManoWar

Artists that are disapproved:

1. Three 6 mafia
2. A2
3. The Dream
4. Birdman
5. Lil Kim
6. Movie Soundtracks
7. Lacuna Coil
8. Man Owar
9. Scar Face

## ATTACHMENT D

DISAPPROVED PUBLICATIONS

<b>December 2010 - January 2012</b>					
<b>Title</b>	<b>Author</b>	<b>Date of Review</b>	<b>Page #</b>	<b>Criteria</b>	<b>Description</b>
Ashley Book of Knots (The)	Clifford W. Ashley	Feb. 22, 2011	entire	C3,C8	instructions to defeat security
1000 Tattoos	ED. Henk Schiffmacher	Oct.21,2011	Entire Book	G	Foreign Language
A Night In A Moorish Harem	H. Douglas	Jan.18, 2011	26	A1	Description of sexual penetration
Academy of Lust	J.Strong	June.30, 2011	16,7,52	A1	Intercourse
Advanced D&D	Player's Handbook	June.30, 2011	entire	G	Written in code
Advanced D&D	Players Handbook Rules Supplement (The Complete Ninja's Handbook)	June.30, 2011	entire	G	Written in code
Advanced D&D 2nd Edition	Players Handbook Rules Supplement (The Complete Thief's Handbook)	June.30, 2011	entire	G	Written in code
Algiers Tomorrow	P.N. Dedeaux	Oct.21,2011	Entire	A3	bondage descriptions
All My Boys	Lindsay Lozon	June.30, 2011	entire	D	Specific information on odds, betting sheets
Al-Minhah Ar-Rabbaaniyyah	?	Jan.18, 2011	entire	G	Entire text printed in foreign language
Al-Qaeda: The Terror Network that Threatens the World	J. Corbin	Sept.6,2011	Throughout	D	depicts violence,disorder, and terrorism
Ambler Warning, The	Robert Ludlum	June.30, 2011	19,20	C5	Information to short out a stun belt
Angels of Death	J. Sher & W.Marsden	Jan.24, 2012	Entire	F	Gang related
Art of Magic and Sleight of Hand, The	N. Einhorn	July. 15, 2011	114	C3	Concealment of weapon
Art of Tantric Sex, The	N. Lacroix	Oct.21,2011	Entire	A1	photos and articles describing sex acts
Bad Girl	M. Reynolds	Aug.10,2011	Entire	A1	Entire book intended for

					sexual acts
Bankers Wife, The	J. Barbour	Dec.10, 2010	92,129,159,160	A1	pictures of actual sexual intercourse
Basics of Biblical Greek: Grammar	William D. Mounce	June.30, 2011	Entire Text Book	G	foreign language
Best Erotic Comics 2008	Greta Christina, editor	June.30, 2011		A1	Intercourse
Billy's Long Game	Bruno Phillips	July. 15, 2011	45	A1	Intercourse
Bin Laden: Behind the Mask of the Terrorist	A. Robinson	Sept.6,2011	Throughout	D	depicts violence,disorder, and terrorism
Black Panther Party Reconsidered, The	Charles E. Jones	Sept.6,2011	Entire	D	Hate Group
Blood & Dishonour	Edited by, N.Wingrove	Aug.10,2011	27	A3	Bondage
Boink: College Sex by the People Having It	the editors of Boink Magazine	June.30, 2011	15,65	A1	Digital penetration of genetalia
Book of Five Rings, The	Thomas Cleary	May. 23, 2011	73,92	C8	
Bride Stripped Bare, The	N. Gemmell	Aug.10,2011	Entire	A1	Entire book intended for sexual acts
Built For Sex	Scott Hays	Jan.18, 2011	58-111	A1	Explicit descriptions and depictions of sexual intercourse
By Appointment Only	Janice Maynard	June.30, 2011	31,35,36,57,58,77,87	A1	Explicit sex scenes - intention of book
Called to the Wild	Angel Blake	Apr. 5, 2011	4,34,35	A	Description of sex acts
Cannabis Cultivator	J. Ditchfield	Aug.10,2011	Through Out	C4	Instructions on how to manufacture drugs
Cheating Wives	Tammy Grainger	Apr. 5, 2011	25, 29	A	Sex Acts
Chemistry For Dummies	John T. Moore Ed.D	May. 23, 2011	278	C4	Ingredients
Chrysanthemum, Rose, and the Samurai	Akahige Namban	May. 23, 2011	68	A3	Bondage
Complete Dirty Laundry Comics, The	A. Kominsky-Crumb, R.Crumb & S.Crumb	Dec.10, 2010	58,56	A1	
Complete Illustrated Kama Sutra	edited by Lance Dane	May. 23, 2011	through out	A1	Depictions of sexual acts

Confessions	S. Vivant and M. Christian	June.30, 2011	#69	A3	Bondage
Continuum	Portia Da Costa	June.30, 2011	17-20,33,38,45	A1	Explicit sex scenes - intention of book
Corruption	Virginia Crowley	May. 23, 2011	8,9	A1,A2	Sexual act & secretion
Crash Out	D. Goewey	Jan.18, 2011	multiple	C1	Escape Techniques
Crave: the seduction of snow white	Cathy Yardley	May. 23, 2011	5,6,7,8,9	A1	Sexual act, penetration
D&D Forgotten Realms	Sons of Gruumsh	Jan.24, 2012	through out	G	Codes
D&D:Diablo II:to Hell and Back	J.Carl,D.Eckelberry,J.Quick,R.Redman	Apr. 5, 2011	entire	G	Coded
D&D:Dungeon Master's Guide II	J.Decker,D.Noonan,C.Thomasson ,J.Jacobs,R.Laws	Apr. 5, 2011	entire	G	Coded
D&D:Epic Level Handbook	A.Collins,B.Cordell,T.Reid	Apr. 5, 2011	entire	G	Coded
D&D:Forgotten Realms: Campaign Setting	Greenwood,Reynolds,Williams,Heinsoo	June.30, 2011	Entire	G	Coded
D&D:Forgotten Realms:Shadowsdale: the scouring of the land	Baker,Boyd,Reid	June.30, 2011	Entire	G	Coded
D&D:Shackled City Adventure Path	multiple	Apr. 5, 2011	entire	G	Codes
D&D:Stronghold Builders Guidebook	M.Forbeck&D.Noonan	Apr. 5, 2011	through out	G	Codes
Defying The Tomb	Kevin "Rashid" Johnson	May. 23, 2011	Entire	F	Gang
Dictionary of Chemistry	Reference	Apr. 5, 2011	8	C4	formulas for potentially toxic substances
Digital Diaries	N. Merritt	Oct.21,2011	Entire	A1, A2	photos intended to show penetration, oral sex, bonding
DocDare	G.Caragonne and G.Morrow	July. 15, 2011	15,28,40,58,86, entire	A1	Promotes & describes sexual activity
Dungeons & Dragons	Dungeon Survival Guide	Oct.21,2011	Entire	G	Codes throughout the book
Dungeons&Dragons	Player's Handbook:Arcan, Divine and Martial Heroes	Nov.21, 2011	24, 25	G	Written in Code
Dungeons&Dragons:Dungeon	T.Cottrill,M.Horne r,C.Youngs	Apr. 5, 2011	through out	G	Codes

Magazine Annual					
Ecstasy, This is	Gareth Thomas	May. 23, 2011	47,52,53,66,47	C4	Ingredients of drug ecstasy
Female Ejaculation	Pokras & Talltrees	June.30, 2011	61 +	A1	Intercourse
Fever Hot Dreams	J.Burton, Sherri L. King, S. Winston	Aug.10,2011	Entire (43,46,etc)	A1	Book is intended to depict sexual acts
Fine Art of Erotic Talk, The	Bonnie Gabriel	Apr. 5, 2011	155	A1	Explicit description of intercourse
Flint Saga,The	Treasure Hernandez	Apr. 5, 2011	16-17	A3	Violent sexual assault described
Forbidden Knowledge Sex	C. Bailey	Feb. 22, 2011	entire	A	sex acts
Game Get Some	Kenya Moore	Apr. 5, 2011	140-141	A	Explicit description of masturbation
Got Fight	Forrest Griffin With Erich Krauss	June.30, 2011	135-188	C8	Instructions to injure, incapacitate
Groove, Bang, and Jive Around	Steve Cannon	May. 23, 2011	164	A1	Sexual act, penetration
Hard Drive	Stanley Carten	June.30, 2011	17,18,19,26,43,49	A1	Explicit sex scenes - intention of book
Heidi's Bedtime Stories	H. Cortez	July. 15, 2011	Entire	A1	Book is intended for sexual encounters
High School Reunion	K. Dean	Oct.21,2011	Entire	A1	sexual descriptions
Highway To Shame	G. Malcolm	Dec.10, 2010	75,221,206	A1, A2	actual sexual intercourse, excretion of bodily fluids
His Fantasies, Her Dreams	Sherri L. King, S.L. Carpenter, T. A. Michaels	Aug.10,2011	Entire (48,73)	A1	Book is intended to depict sexual acts
Holy War, Inc.	Peter L. Bergen	Sept.6,2011	Throughout	D	depicts violence,disorder, and terrorism
Hot Cheeks	edited by M. Sigrist	Aug.10,2011	49	A1	Digital Penetration of genitalia
Hot Nurse's Nympho Sister, The	Irene Troon	May. 23, 2011	81-82	A1	Sexual act, penetration
House of Dreams: Book II	Michael Hemmingson	May. 23, 2011	10,11	A1	Penetration
Hunt for the Engineer, The	Samuel M. Katz	Sept.6,2011	Throughout	D	depicts violence,disorder, and terrorism
I Am the Market	L. Rastello	Aug.10,2011	Entire	D	promotes breaking laws of drug smuggling

In Bed With	mutiple authors	Jan.24, 2012	64, 78, 195, 197	A1	sexual descriptions
In the Name of Osama Bin Laden	R. Jacquard	Sept.6,2011	169 - end	G	Foreign Language
Island Girls: Tropical Lesbian Erotica	edited by: S. Thorne	Oct.21,2011	Entire Book	A1	sexual descriptions
Key of Solomon the King, The	Mathers	July. 15, 2011	multiple	G	Hebrew, Codes
Killing Johnny Fry	Walter Mosley	Apr. 5, 2011	17-19,42,45,207,212,232	A1	Entire book is intended for graphic sex.vivid descriptions of sexual penetration
Kiss Kompendium: The First Complete Collection		Oct.21,2011	Entire	H	Size
Kiss, The	Hans-Jurgen Dopp	Jan.18, 2011	multiple	A1	Description of sexual penetration
Knowledge of Self	Dr.Supreme Understanding Allah C'BS Alife Allah	Feb. 22, 2011	131-173	F	gang related material
Law of Nines, The	Terry Goodkind	June.30, 2011	137 +	A3,D	Bondage, Violence
Lawyer,The	M.Hemmingson	Aug.10,2011	Entire	A	Books primary purpose promotes sexual acts/conquests
Learn To Read The Qur'an		June.30, 2011	entire	G	Material written in foreign language with no translation
Learning to Love it	A.Tyler	Aug.10,2011	Entire	A1	The intention of book is for sexual depictions
Letters To Penthouse	XXXV	July. 15, 2011	Entire	A1	Book promotes sexual activity
Letters To Penthouse	XV	July. 15, 2011	49,50,52,53,103,105, entire	A1	Book is intended for sexual encounters
Letters To Penthouse	X	July. 15, 2011	Entire	A1	Book is intended for sexual encounters
Letters To Penthouse	XXX	July. 15, 2011	Entire	A1	Book is intended for sexual encounters
Letters To Penthouse	XXII	July. 15, 2011	Entire	A1	Book is intended for sexual encounters
Letters To Penthouse	XXI	July. 15, 2011	Entire	A1	Book is intended for sexual encounters
Letters To Penthouse	XXXVI	May. 23, 2011	Entire	A1	Entire book is geared towards sexual acts and descriptions

Letters To Penthouse	XXXIV	May. 23, 2011	Entire	A1	Entire book is geared towards sexual acts and descriptions
Letters To Penthouse	VIII	May. 23, 2011	Entire	A1	Entire book is geared towards sexual acts and descriptions
Letters To Penthouse	XXXVII	May. 23, 2011	Entire	A1	Entire book is geared towards sexual acts and descriptions
Letters To Penthouse	XXIX	May. 23, 2011	Entire	A1	Entire book is geared towards sexual acts and descriptions
Life in the World of Women	Maxim Jakubowski	May. 23, 2011	17	A1	Penetration
Lip Service	Don and Debra Macleod	Feb. 22, 2011	entire	A	sex acts
Living In the State of Dreams	M. Millswan	June.30, 2011	128	A1	Penetration
Lost Fighting Arts of Vietnam	Dr. Haha Lung	May. 23, 2011	Entire	C8	step by step instructions and illustrations for using deadly techniques and tactics
Love on the Dark Side	various	Oct.21,2011	Entire	A1	Intent of entire book is sex. Descriptions of sexual intercourse
Mafia	US Treasury Dept. Bureau of Narcotics	Jan.18, 2011	entire	F	Profiles of Mafia members
Mammoth book of New Erotic Photography, The	Edited by M. Jakubowski	July. 15, 2011	211,16,32	A1	Intercourse
Mammoth Book of Secret Codes and Cryptograms, The	E. Dunin	June.30, 2011	Entire	G	Codes
Man Slave	J D Jensen	May. 23, 2011	18,19,45	A3	descriptions of bondage, violent acts
Mana Suenos Liquidos		Dec.2, 2011	Entire	G	Entire text is in Spanish
Martyrs	Joyce M. Davis	Sept.6,2011	Throughout	D	depicts violence,disorder, and terrorism
Mastering Jujitsu	Gracie	June.30, 2011	entire	C8	photos, instructions to



					restrain/injure
Mating Game	Janice Maynard	June.30, 2011	13,14,23,63	A1	Explicit sex scenes - intention of book
McMafia	Misha Glenny	Apr. 5, 2011	Entire	D	Dissection of organized crime and activities
Messy Girls	C. Gatewood	Feb. 22, 2011	321,331	A	sexual act, sucking breast
More Forbidden Knowledge	Matt Forbeck	Apr. 5, 2011	37,43,multiple	C4,C5	Instructions on how to make beer, how to remove hand cuffs
Mortal Seductions	A. James	Aug.10,2011	Entire	A1	The intention of book is for sexual depictions
New Testament	translated by: W.Tyndale	June.30, 2011	entire	G	Language can not be deciphered, wording can not be read
Nina Hartley's Guide to Total Sex	N.Hartley with I.S. Levine	Feb. 22, 2011	entire	A	sex acts
Notebooks of Madame B: Seduction, The	Madame B	Jan.24, 2012	Entire	A1	descriptions of sexual acts
One More Time	Celia May Hart	Jan.24, 2012	multiple	A1	descriptions of sexual acts
Open for Business	A. Tyler	Jan.24, 2012	multiple	A1	descriptions of sexual acts
Oxford Comprehensive Atlas of the World	Reference Book	June.30, 2011		H	Exceeds size dimension limit of 11X14
Pathfinder	Rise of the Runelords: Player's Guide	Dec.2, 2011	5, 7	G	Written in Code
Pathfinder	Curse of the Crimson Throne: Player's Guide	Dec.2, 2011	13	G	Written in Code
Pathfinder	Advanced RolePlaying Game	Jan.24, 2012	Entire	G	written in code
PathFinder: Role Playing Game	Bestiary 2	Dec.2, 2011		G	Codes
PathFinder: Role Playing Game	Ultimate Magic	Oct.21,2011	Entire Book	G	Codes throughout the book
PathFinder:King Maker: War of the River Kings	J.Nelson	Oct.21,2011	Entire	G	Codes throughout the book
PathFinder:King Maker:Blood for Blood	N. Spicer	Oct.21,2011	Entire	G	Codes throughout the book

Pathfinders: A Gamemastery Adventure Path	Curse of the Crimson Throne: Seven Days to the Grave	Dec.2, 2011	79	G	Codes
Pathfinders: A Gamemastery Adventure Path	Curse of the Crimson Throne: Escape From Old Korvosa	Dec.2, 2011	Multiple	G	Codes
Pathfinders: Campaign Setting	Lost Cities of Golarion	Dec.2, 2011	Throughout	G	Codes
Pill Book, The	New and Revised 13th Edition	Sept.6,2011	Entire	C4	Ingredients of drugs
Pimpology	Pimpin' Ken	July. 15, 2011	Entire	D	Promotes criminal activity
Please Sir	Rachel Kramer Bussel	June.30, 2011	71	A3	Violent Sex Acts
Pleasure Control	Cathryn Fax	Apr. 5, 2011	23-46,48-51,104, various	A1,A3	Graphic depictions of sex acts(intent of book),bondage of hands
Plot&Poison:A Guidebook to Drow	Races of Renown	Dec.2, 2011	55, 69	G	Written in Code
Pornoland	S. De Luigi & M.Amis	Feb. 22, 2011	70, end	A1	penetration
Prodigal Father-Pagan On	A. Menginie & K.Droban	Jan.24, 2012	Entire	F	identified STG group
Purple Pillow Book	Dee McDonald	June.30, 2011	37,38,94	A1	Depiction of actual sexual intercourse
Ravished American Bride(The)	B. Stainer	Feb. 22, 2011	43,100,204	A1,A2	pictures of sexual acts, secretions
Real Goon's Bible, A	Derrick Johnson	May. 23, 2011	4,36,37,59,82,107,117,120	D,F	pages identified and entire book is geared towards gang violence and depictions
Reckoning, The	Anonymous	Apr. 5, 2011	46,70,71, various	A1,A3	Sexual Acts:using fingers and objects to penetrate. Sadistic beatings. Intent of book:sexual
Rio Erotico	O. Stupakoff	Oct.21,2011	60-61	A1	Digital Penetration
Satanic Bible, The	Anton Szandor LaVey	Dec. 2011	117,118,149,88,89	D, E	promotion of violence, detrimental to rehabilitave efforts
Secret Art of Boabom, The	Asanaro	Jan.24, 2012	Entire	C8	information to injure
Seduce Me	D. Schweitzer	July. 15, 2011	Entire	A1	Book is intended for sexual encounters
Seeds of Terror	Maria A. Ressa	Sept.6,2011	Throughout	D	depicts

		11	t		violence,disorder, and terrorism
Sensualists, The	Frank Mace	Apr. 5, 2011	15	A, A3	Sex Acts
Sex Advice From....	the Editors of Nerve.com	Feb. 22, 2011	entire	A	sex acts
Sexual Astrology	Martine	Apr. 5, 2011	123	A1	Explicit description of sexual acts
Sexual Criminal, The	J. Paul De River	June.30, 2011		A3	bondage, sadistic material
Sexual Reflexology	Chia and Wei	May. 23, 2011	Entire	A1	Sex Acts, Penetration
Shameful Duties	S. Saraband	Feb. 22, 2011	35,69,121, 168	A1	inanimate object penetration, sexual penetration
Shaolin Workout, The	Sifu Shi Yan Ming	June.30, 2011		C8	Instructions to Disable
She Comes First	Ian Kerner, Ph.D.	May. 23, 2011	Entire	A1	Vivid descriptions of sexual acts
Skin Deep	Anna J. Evans	June.30, 2011	43-44,73- 75,95	A1	Explicit sex scenes - intention of book
Slow Hand	M. Slung	Dec.10, 2010	120,380,6 0,61,109	A1	explicit depiction of sexual act
Sneakiest Uses for Everyday Things	C.Tymony	Oct.21,20 11	Entire Book	C1,3,5	Information to alter articles and objects
Something Reckless	J.Michaels	Aug.10,20 11	Entire	A1	The intention of book is for sexual depictions
Spicy Bedtime Companion, the	Joan Elizabeth Lloyd	June.30, 2011	63,87	A1	Penetration
Star Wars: Role Playing Game	Saga Edition:Revised Core Rulebook	Apr. 5, 2011	entire	D,G	Depictions of violence, codes used
Star Wars: Role Playing Game	Force Unleashed- Campaign Guide	June.30, 2011	Entire	G	Coded
Star Wars: Role Playing Game	Legacy Era: Campaign Guide	June.30, 2011	Entire	G,D	Coded, Violence
Star Wars: Role Playing Game	Clone Wars: Campaign Guide	June.30, 2011	Entire	G	Coded
Star Wars: Role Playing Game	Unknown Regions	June.30, 2011	Entire	G	Coded
Star Wars: Role Playing Game	Rebellion Era Campaign Guide	June.30, 2011	Entire	G	Coded
Star Wars: Roleplaying Game	Scum and Villainy	Oct.21,20 11	Entire	G	Codes throughout the book
Stare	D. Ridgers	Feb. 22, 2011	entire	G	foreign language
Stella Does Hollywood	Stella Black	June.30, 2011	44	A3	Graphic Description of bondage
Strategists & Tacticians	R. Costello, Jr.	Dec.10, 2010	54,63	C8	combat, kill tactics

Street Legends: Vol.1	S. Ferranti	Oct.21,2011	Entire Book	D,F	book about street gangs, gang signs,violence,criminal activity
Street Legends: Vol.2 OGS	S. Ferranti	Oct.21,2011	Entire Book	D	book intention: describes gang activities and violence
Sun Stroked	C. Fox	Oct.21,2011	57,61,75	A1	Depiction of Sexual acts, book of erotic escapades
Supreme Lessons of the Gods and Earths	compiled by, God Supreme Allah	Jan.24, 2012	Entire	F	material promoting gangs. Lessons for five percenters
Swords&Sorcery	Arcana Unearthed	Jan.24, 2012	Entire	G	written in code
Taming The Beast	Emily Maguire	May. 23, 2011	96	A1	Sex Acts, Penetration
Taoist Foreplay	Mantak Chia and Kris Deva North	June.30, 2011	119	A1	Penetration
Teach Yourself Electricity and Electronics: Fourth Edition	Stan Gibilisco	June.30, 2011	Entire	C5	Alter, defeat electronics
Thai Honey	Kit McCann	Jan.18, 2011	172-173	A2, A3	Fluid, Bondage
Third Imperium, the	Tripwire (MGP 3820)	Jan.24, 2012	Entire	G	written in code
Third Imperium, the	Alien Module 3: Darrians	Jan.24, 2012	Entire	G	written in code
Third Imperium, the	Alien Module 2: Vargr	Jan.24, 2012	Entire	G	written in code
Third Imperium, the	Alien Module 1: Aslan	Jan.24, 2012	Entire	G	written in code
This Will Kill You	HP Newquist and Rich Maloof	June.30, 2011	112,133 +	C8	Instructions to disable
Tokyo Story	Akahige Namban	May. 23, 2011	5,6 +	A1	Penetration
Transgressions	Erastes	Aug.10,2011	Entire	A1, B	Sexual depictions; sexual depictions with children
Ultimate Guide to Cunnilingus, The	V. Blue	Jan.24, 2012	through out	A	sex acts
Ultimate Guide to U.S. Special Forces, The	J. McCullough	Sept.6,2011	entire book	C3,C4, C8	
Ultimate Warrior Workouts	M. Rooney	May. 23, 2011	23,entire book	C8	descriptions/depictions of training exercises in preparation for martial arts that could be used to injure,disable, or

					kill a person
Unofficial Guide to Ethical Hacking, The	Ankit Fadia	Apr. 5, 2011	entire	C.5	
Venus In India	Charles Devereaux	June.30, 2011	41,97,98,111	A1	Explicit sex scenes - intention of book
Venus In Lace	Marcus Van Heller	May. 23, 2011	109	A1	Penetration
Vietnamese Bible		May. 23, 2011	entire	G	entire texts in foreign language without translation
Violetta	Stan Kent	May. 23, 2011	11	A1, A3	Penetration, Bondage
Vitamin O	Dr. Natasha Janina Valdez	Oct.21,2011	Entire Book	A1	Sexual act descriptions and stimulations
What Women Really Want in Bed	C. Gentry & Fredsti	Feb. 22, 2011	numerous	A	sex acts
Where the Girls Are	edited by, DI King	Oct.21,2011	Entire	A1	Intent of book is sexual acts and descriptions
Wilderness Survival Handbook	Pewtherer	May. 23, 2011	various	C3	manufacture of weapons,cages, traps
Women onTop	Nancy Friday	May. 23, 2011	79	A1	Penetration
Zarqawi	Jean-Charles Brisard w/ Damien Martinez	Sept.6,2011	216, throughout	D,G	depicts violence, disorder, and terrorism, foreign language

## ATTACHMENT E


CURRENTLY PARTICIPATING FACILITIES

<u>Facility</u>	<u>Region</u>	<u>Average Daily Population</u>
Sussex	Eastern	1,116
Sussex II	Eastern	1,270
Keen Mountain	Western	894
Red Onion	Western	642
Wallens Ridge	Western	1,037
Nottoway	Central	1,193
		6,152 Total

**ATTACHMENT F****SECURITY REQUIREMENTS**

1. The Contractor shall be responsible for ensuring that all personnel, equipment, tools and supplies/materials comply with any and all rules, regulations, and procedures of the Agency and the individual facilities. Questions should be addressed to the on-site Business Manager or a member of the administrative staff at each facility. The individual facility's rules, regulations and procedures governing the entry and conduct of staff working inside the facility will be made available and explained at the point of entry. The Department of Corrections reserves the right to deny entrance to anyone who is suspected of a breach of security or for failure to follow published rules, regulations or procedures.
2. All personnel entering a correctional facility will be subject to a search of their person and personal items. Such searches may be frisk searches, searches by metal detectors or searches by narcotics detection canines. In addition, all equipment, tools, supplies and materials will be subject to search or inventory at any time. Tools and materials must be carefully controlled at all times and locked when not in use. All ladders and movable lift equipment must be closely supervised when in use and brought out of the security compound when not in use.
3. Any attempts to introduce contraband, to assist in escape, or to have unauthorized contact with offenders or wards of a facility are prohibited and will be prosecuted under the provisions of the Code of Virginia. The Contractor's personnel are prohibited from bringing into or taking out of the institution any items unless specifically approved. Any interaction between a Contractor's employee and an offender, which assists the prisoner to escape, is a felony and will be prosecuted. Contractor's personnel may not deliver, receive or otherwise transfer **any item**, no matter how harmless, to or from an offender without express permission of the Warden/Superintendent or designee.
4. Contractor's personnel or representatives are limited to movement to, from and within their assigned work area. No contact is allowed with offenders unless expressly approved.
5. No person who appears to be under the influence of drugs or alcohol will be allowed entry into a correctional facility.
6. All Contractors' personnel must be in possession of a valid identification with a recent, clear photo in order to enter a facility. All Contractors' personnel are required to be dressed appropriately for the duties they are performing. The Contractor's personnel shall not wear any clothing that is similar to or could be mistaken for an offender uniform. Clothing that is short, tight-fitting, or revealing is not appropriate attire for a prison environment. Individuals so dressed will be asked to change their clothing or leave the facility.
7. Any mail or packages received at the facility will be searched prior to being delivered inside the security perimeter.
8. The entrance of vehicles or motorized equipment inside the security perimeter is discouraged. However, should this be required, any vehicle left unattended must be locked and the keys removed or it should be otherwise rendered inoperable. No vehicle is permitted to leave the security perimeter until an institutional count has been completed. Count times will vary.

## ATTACHMENT G

	<h1>Operating Procedure</h1>	<b>Effective Date</b> October 1, 2011	<b>Number</b> 310.2
		<b>Amended</b> 10/5/11, 1/12/12, 2/22/12, 3/9/12, 4/30/12, 5/15/12, 8/13/12, 8/28/12, 11/2/12, 2/1/13, 8/16/13, 9/26/13	<b>Operating Level</b> Department
		<b>Supersedes</b> Operating Procedure 310.2 (7/1/10)	
		<b>Authority</b> COV §53.1-10, §2.2-2010, §2.2-2651, §2.2-2827	
<b>Subject</b> <b>INFORMATION TECHNOLOGY SECURITY</b>		<b>ACA Standards</b> 4-4100, 4-4101, 4-4102; 4-ACRS-7D-05, 4-ACRS-7D-06	
<b>Incarcerated Offender Access</b> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	<b>FOIA Exempt Attachments</b> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> #2	<b>Office of Primary Responsibility</b> Chief Technology Officer	

## I. PURPOSE

This operating procedure establishes security controls in accordance with Commonwealth of Virginia Information Technology Resource Management Information Security Standard COV ITRM Standard SEC501-06. This standard defines the requirements to protect Department of Corrections data and information from loss, unauthorized use, modification, disclosure, or reproduction, and to ensure the implementation of, and compliance with, controls, standards, and procedures. This operating procedure ensures that all data and information, and the means by which they are created, gathered, processed, transmitted, communicated, and retained are identified, classified, controlled, and safeguarded. DOC data and information must also meet federal, state, and other regulatory and legislative requirements.

## II. COMPLIANCE

This operating procedure applies to all units operated by the Department of Corrections (DOC). Practices and procedures shall comply with applicable State and Federal laws, Board of Corrections policies and regulations, ACA standards, and DOC directives and operating procedures.

This operating procedure applies to all DOC employees, contractors, volunteers, and partners requiring access to or the use of DOC Information Technology Resources. Employee failure to follow this procedure is a violation of Operating Procedure 135.1, *Employee Standards of Conduct*, and may result in disciplinary action.

## III. DEFINITIONS

**Administration and Operations Manager** – The head of the Fiscal Administration and Operational section of CTSU

**Agency Information Technology Resources (AITR)** – Liaison between the agency and VITA to



ensure that information (questions, concerns, issues, etc.) flow smoothly between the two parties and the right people are involved in the communication process.

**Case Sensitive** - A computer program's ability to distinguish between uppercase (capital) and lowercase (small) letters. Programs that do not distinguish between uppercase and lowercase are said to be case insensitive.

**Chief Technology Officer (CTO)** - The head of the DOC Corrections Technology Services Unit.

**Corrections Technology Services Unit (CTSU)** – A unit established within the Department of Corrections to manage information technology services for the DOC.

**CTSU Security** - The information security section within the CTSU unit - The Information Security Officer (ISO) is the head of CTSU Security.

**Data** - Includes but is not limited to, information in a database, application and operating system (OS) software, operational procedures, system design, organization policies, system status, and personnel schedules.

**Data Custodian** – Individual responsible for physical or logical possession of DOC IT system data. The custodian monitors and operates systems appropriately and protects the data from unauthorized access, modification and destruction. Provides reports to the Data Owner as required.

**Data Owner** – Manager responsible for policy, procedure, and practice decisions regarding data sensitivity, access, and protection on a DOC IT system.

**Information Security Officer (ISO)** - The head of CTSU Security

**Information Technology (IT)** - Equipment or interconnected system or subsystem used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services and related resources.

**Information Technology Initiative** - Any software development or purchase, network deployment including utilizing solutions such as Internet access or wireless technology, and hardware deployment

**Internet** - A global collection of interconnected computer networks sharing a wide variety of resources (research and archived data, publications, news, weather, electronic mail, etc.) and functionality including “e-government”, communications, and entertainment. No one individual is in charge of, or owns, the Internet. Internet Service Providers (ISP s) offer the vehicle for access to the Internet.

**IT Infrastructure Partnership** - Information technology management and services provided to Virginia State Government by Virginia Information Technologies Agency (VITA) and Northrop Grumman (NG).

**Local Site Support (LSS)** - An individual whose primary responsibilities are not related to IT, but

provides IT support to others within the same operating unit (e.g. VACORIS).

**Malware ("malicious software")** – Programs or files designed to infiltrate and damage a computer system without the owner’s knowledge. Malware includes computer viruses, worms, Trojan horses, rootkits, spyware, some adware, malicious, and unwanted software. (*Also see Virus, Worm*)

**Non-DOC requests** - Software application requests by government agencies (State, local and federal) that have a valid need to access DOC software applications (e.g. VACORIS).

**Northrop Grumman (NG)** - Contract vendor responsible for the service delivery of the Commonwealth's IT infrastructure needs, with oversight from VITA.

**Obscene Material** - Any material that “considered as a whole, has as its dominant theme or purpose an appeal to the prurient interest in sex, that is, a shameful or morbid interest in nudity, sexual conduct, sexual excitement, excretory functions or products thereof or sadomasochistic abuse, and which goes substantially beyond customary limits of candor in description or representation of such matters and which, taken as a whole, does not have serious literary, artistic, political or scientific value.”

**Offender** - Inmate, Probationer, Parolee, or Postreleasee under the supervision of the DOC.

**Organizational Unit Head** - The person occupying the highest position in a DOC operating unit, such as a correctional facility, probation and parole district, regional office, or a separate operational unit in the DOC central headquarters including the offices of the Director and Deputy Directors

**PC** - Personal computer, which also applies to all DOC workstations, including laptop computers.

**Security Incident** - Any act or circumstance that compromises, harms, or destroys DOC software, hardware, or data

**Sensitive Data** – Information whose worth is calculated based on its value to the owner

**Social Media** – Form of online communication or publication that allows for multi-directional interaction. Social media includes: blogs, wikis, podcasts, social networks, photograph and video hosting websites and new technologies as they emerge.

**Social Networking** – Interacting with a group of people with common interests in a virtual environment.

**Software Applications** - Software used by DOC personnel to perform needed job duties (e.g. VACORIS, CARS, FAACS, *Inmate Pay / Inmate Trust, etc.*).

**Software Applications Authorizer** - The “owner” of a software application relating to DOC business. This individual approves access rights and privileges to DOC applications (e.g. VACORIS, CARS, *etc.*).

**System Administrator** – Analyst, engineer, or consultant responsible for implementing, managing, or operating a DOC IT system at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator manages day-to-day administration and implements security controls and other requirements of DOC IT systems.

**System Owner** – Manager responsible for operation, maintenance, and documentation of risk for a DOC IT system.

**User ID** - The name given to a user or account that enabling access to the computer system/network.

**Virginia Information Technologies Agency (VITA)** - Central management of the Commonwealth’s information technology resources, counterpart of CTSU.

**Virtual Memory System (VMS)** - References the root account from which users gain access through the Gateway to software applications residing on either the VAX (*Inmate Pay / Trust, POS, etc.*) or VITA (*CARS, LIDS, etc.*).

**Virus** - A program which can replicate itself and infect a computer without the user’s knowledge. The difference between a virus and a worm is that a virus requires a host program in order to replicate. A virus can only spread from one computer to another when its host is taken to an uninfected computer and spread to other computers by means of a network file system, USB, CD, etc., then accessed by other computers. For a virus to replicate, it must be permitted to execute code and write to memory. This is the reason, many viruses attach themselves to executable files which are part of legitimate programs. (Also see *Malware, Worm*)

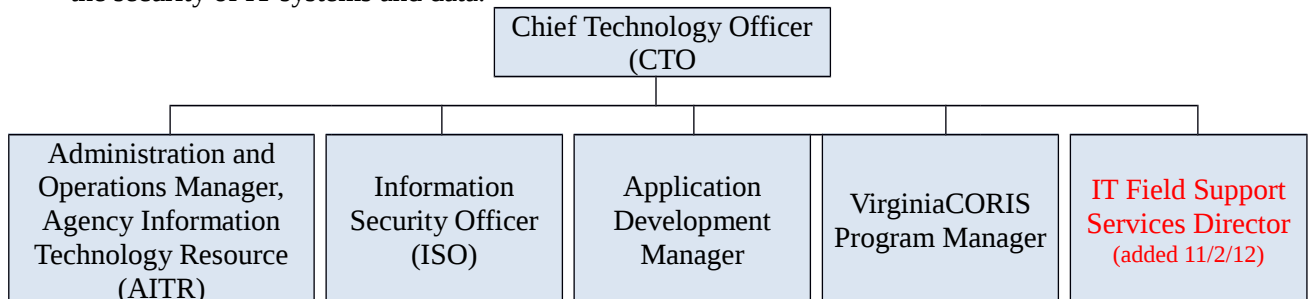
**Wireless IT Equipment** –Equipment, including 802.11 a/b/g and Bluetooth or any equipment connecting to or interacting with DOC information technology systems without the use of wires such as: wireless access points, wireless cards, cellular cards or phones used to access other networks while connected to the DOC’s network, handheld PCs and personal information managers utilizing Bluetooth or 802.11 a/b/g to access any network while still connected to the DOC network.

**Workstation** - The device used by employees to connect to the network or system resources. Workstation also means personal computers and laptop computers.

**Worm** – A self replicating computer program which uses the computer network to send copies of itself to other computers attached to the network, without any user intervention. Unlike a virus, a worm does not need to attach itself to an existing program, meaning it can spread itself to other computers without needing to be transferred as part of a host. A worm does its damage by spreading through the network exploiting vulnerabilities in operating systems and almost always causing harm to the network. (Also see *Malware, Virus*)

IV. ORGANIZATIONAL RESPONSIBILITIES

A. The following organizational chart depicts the reporting structure within CTSU responsible for the security of IT systems and data.



B. The Chief Technology Officer (CTO) of the Corrections Technology Services Unit is responsible

- for security of DOC information technology resources.
- C. The CTO shall approve all DOC software applications development to be used by multiple users. There are NO exceptions. Applications created or installed without this approval will not be supported by CTSU and may be required to be uninstalled.
  - D. The DOC Information Security Officer (ISO) shall implement and maintain the DOC information security program.
    - 1. The ISO shall ensure that adequate and appropriate levels of protection for DOC technical resources are in place to prevent unauthorized or unnecessary access or disclosure, and ensure effective and accurate processing and continuity of operations as relates to Information Technology security within the DOC.
    - 2. The ISO shall create, implement, enforce, and maintain security policies, procedures, and IT security programs for DOC Information Technology resources and systems under the direction of the CTO.
    - 3. The ISO may appeal directly to the Deputy Director for Administration for review and resolution of a security issue or concern that the Chief Technology Officer has not properly addressed or prioritized.
    - 4. The ISO shall maintain liaison with the Chief Information Security Officer of the Commonwealth.
  - E. The Administration and Operations Manager provides oversight of operational technology activities to include routing, switching and telecommunications in support of institutions and community corrections as well as the maintenance of IT asset inventory and software licenses. Administration functions include billing, procurement, transfer and disposal of assets.
  - F. The Agency Information Technology Resource (AITR) is responsible for ensuring cooperative sharing of information between the agency and VITA.
  - G. The Application Development Manager is responsible for all custom application development as well as database administration, ensuring security standards, guidelines and procedures are adhered to.
  - H. The IT Infrastructure Partnership (VITA/NG) shall configure and deploy all DOC servers and workstations not identified by the ISO as being related to security. Servers and workstations will be configured in accordance with the VITA/NG server and workstation standard configuration procedures. ISO designated security servers are supported solely by the ISO and other security staff. VITA/NG is responsible for all contracted hardware maintenance.
  - I. Organizational Unit Heads shall ensure that policies and procedures relative to information technology security are enforced in accordance with this operating procedure.
  - J. In order to complete the annual IT Security Awareness Training requirements, all salaried and wage employees, consultants, volunteers and authorized users having a DOC IT system account are required to read and consent to the terms of the DOC Information Security Agreement.
  - K. All VITA/NG staff, and individuals included in the Windows Domain Administrator Group, will sign the [Windows Admin/System Security Agreement](#) 310\_F1.
- V. ACCESS TO DOC INFORMATION TECHNOLOGY RESOURCES
- A. VITA/NG is designated and responsible for all DOC System account maintenance and activities (additions, deletions, transfers, renames, disk quota allocations, etc.).

1. VITA/NG is responsible for monitoring all accounts for adherence to this procedure and all other relevant codes, laws, and policies applicable to DOC Information Technology.
  2. CTSU Security will review these activities for compliance.
- B. Requests for account maintenance and activities shall be communicated to ~~the DOC CTSU Security Office. VITA/NG through the Virginia Customer Care Center (VCGG).~~ (changes 2/22/12)
1. Accounts must be granted on the basis of least privilege. The principle of least privilege requires that access is only provided to the systems that are required of the user to complete their functions.
  2. Account requests are managed as follows:
    - a. All new user account requests must include a [Windows/VMS User Account Request](#) 310\_F2 submitted to ~~CTSU Security the VCGG.~~
    - b. Each request for a new account must include a [Windows/VMS User Information Security Agreement](#) 310\_F3 signed by the user. This shall be kept in the user's personnel file locally.
    - c. All requests for a VMS accounts must include a [Windows/VMS User Account Request](#) 310\_F2 submitted to ~~CTSU Security the VCGG.~~
    - d. All user re-name account requests must include a [Windows/VMS User Account Request](#) 310\_F2 submitted to ~~CTSU Security the VCGG.~~
    - e. All requests for account transfers must be submitted by the receiving location utilizing a [Windows/VMS User Account Request](#) 310\_F2 to ~~CTSU Security the VCGG.~~
    - f. All requests for account disables must include a [Windows/VMS User Account Request](#) 310\_F2 submitted to ~~CTSU Security the VCGG.~~
    - g. Any user going on a leave of absence expected to last 30 days or more must have their account disabled for the duration of their absence.
    - h. For an account to be re-enabled, the user's Supervisor, Human Resources Officer (HRO), or CTSU Security must make the request by e-mail or by telephone. *A form is not required to re-enable an account.*
    - i. All requests for account deletions must include a [Windows/VMS User Account Request](#) 310\_F2 submitted to ~~CTSU Security the VCGG~~ by the user's Supervisor.
    - j. Requests to disable an account must be submitted to ~~CTSU Security in a timely manner after the VCGG within 24 hours of~~ an employee or contractor termination. (changed 8/16/13)
  3. Guest and shared accounts are prohibited on sensitive systems.
  4. All VITA/NG staff, and individuals included in the Windows Domain Administrator Group must request Admin/System Accounts by submitting a [Windows Admin/System Account Request](#) 310\_F4 to ~~CTSU Security the VCGG.~~ A signed copy of the [Windows Admin/System Security Agreement](#) 310\_F1 should be sent to CTSU Security.
  5. Requests for access to shared folders must be submitted to CTSU Security, defining the specific access required. For example: the name of the shared folder and the type of access needed. To be written similar to: `\\s3groups\James River\Dairy` Modify or Read only access (added 4/30/12)
  6. Access to another user's information (mail or shared folders) must be submitted to CTSU Security. (added 4/30/12)

- C. Accounts must be validated periodically to determine if the access is still necessary
1. VITA/NG and CTSU Security will monitor account usage. Accounts that have not been logged into after 90 days will be disabled. After 120 days of inactivity, accounts may be deleted upon request of the business unit contact.
  2. VITA/NG must also conduct a review of all Domain Admin, Server Admin, and System accounts. Accounts not being utilized within 90 days should be deleted.
  3. For actions warranting disciplinary suspension greater than one day, accounts and physical access must be disabled.
- D. Remote Access (~~CISCO AnyConnect Firepass~~) (changed 11/2/12)
1. ~~Remote access via the IT Partnership enterprise solution (CISCO AnyConnect) is provided to all users and is installed on all devices. Remote access (Firepass) should not be granted except for a legitimate business purpose, and authorization is required by the user's Organizational Unit Head using Remote Access to DOC Applications and IT Resources 310\_F5 sent to CTSU Security.~~
  2. ~~CISCO AnyConnect Access All remote access (Firepass) should use 128-bit or greater encryption.~~
    - a. Users who previously had Firepass access will have the permissions for AnyConnect added to their account. No request or forms are necessary.
    - b. The organizational unit head will need to submit an email to CTSU Security to request new AnyConnect users to be added to the VPN group. No form is necessary.
  3. Use of any remote connection to DOC IT Systems constitutes acceptance of and agreement to this operating procedure. Remote connections to DOC IT Systems may be monitored, scanned, or analyzed at any time without notification or consent.
  4. All remote connections to DOC IT Systems should be originated from a DOC owned device excluding authorized contractors with approved equipment.
  5. All systems connected to the DOC IT Systems remotely must be running virus protection with current virus definitions.
  6. All systems connected to the DOC IT Systems remotely must be up to date on all current operating system and software security hot fixes, service packs, patches, and updates.
  7. Those not in agreement with this operating procedure and its conditions should not connect to DOC IT Systems.
  8. All systems connected to the DOC IT Systems remotely must utilize a firewall to protect the DOC from any other systems the device originating the remote connection may be connected to.
- E. Non-DOC Requests for Access to DOC IT Systems
1. ~~This type of access is provided utilizing the IT Partnership enterprise solution SWAP (Secure Web Access Portal).~~ (added 11/2/12)
    - a. All initial requests by non-DOC users for access to DOC software applications or systems must be submitted in writing to the CTO or to CTSU Security. The requestor must submit clear justification for the need for access to the DOC Systems. Once approved by the CTO CTSU Security will notify the requestor when access is granted. The request must include

the following information:

- i. The type of access required
  - ii. Direction of dataflow
  - iii. Contact information for the organization owning the IT system and/or data, including the System Owner and System Administrator.
  - iv. There shall be a written agreement delineating the security requirements for each interconnected IT system and each type of data shared. All future connectivity must be established in the written agreement before implementation can occur.
  - v. The written agreement shall also include data handling, storage, and disclosure.
2. The non-DOC requestor is responsible for notifying CTSU Security of removal of access privileges when access is no longer needed. Failure to comply with this paragraph may result in denial of future requests.
  3. The non-DOC requestor will be provided a copy of this operating procedure. Use of granted access constitutes acceptance and agreement to abide by this operating procedure.
  4. ~~Non-DOC entities that are granted access are required to sign a [Windows/VMS User Information Security Agreement 310\\_F3](#). (deleted 3/9/12)~~
  5. Non-DOC entities that are granted Domain Administrator Access must sign the [Windows Admin/System Security Agreement 310\\_F1](#).

#### F. Software Application Authorization and Revocation

1. Acceptable access to DOC software applications and non-DOC software applications are contingent upon approval by the requestor's supervisor and the Software Applications Authorizer.
2. ALL requests for access to DOC software applications (*VACORIS, Inmate Pay / Trust, etc.*) or non-DOC software applications (*CARS, LIDS, CAIS, etc.*) must be sent to and approved by the Software Applications Authorizer listed on the *DOC Applications Access Authorization* (see Attachment 1). (4-4100, 4-4102, 4-ACRS-7D-05, 4-ACRS-7D-06)
  - a. It is the responsibility of the authorizer to notify CTSU Security of authorized designee additions and deletions.
  - b. Questions concerning the authorization list should be directed to the CTSU mailbox: (CTSUSecurity@vadoc.virginia.gov).
3. No requests for access to software applications are to be sent directly to the VCCC, nor will they be accepted. The Software Applications Authorizer is responsible for notifying CTSU Security of requests and authorizations for access.
4. CTSU Security will accept the following valid application authorization requests from the Software Applications Authorizers' and their designees:
  - a. E-mail from the Software Applications Authorizer or their designee.
  - b. Written correspondence with a valid authorization signature from the Software Applications Authorizer or their designee
5. CTSU Security will accept the following requests for revocation of privileges:
  - a. E-mail or written correspondence from DOC managing supervisor
  - b. The ONLY exception is a request from DOC Special Investigations Unit or DOC

management, due to an investigation or urgent need. All such urgent requests must be backed up with written authorized correspondence for documentation purposes.

6. ~~VITA/NG must notify CTSU Security of all account deletions and transfers via VCCC ticket.~~ CTSU Security will remove all software application access for account deletions and determine if software application access removal is necessary for account transfers. (deleted 4/30/12)
7. ALL software application privileges granted, modified, and/or revoked must be performed by the CTSU Security group or their designee.

## VI. USAGE OF DOC INFORMATION TECHNOLOGY RESOURCES

### A. Network Login Banner and Authorized Login Accounts

1. VITA/NG will ensure the *Logon Banner* (see Attachment 2) is implemented within the login script for all workstations, servers connected to the network, and standalone devices. The banner will be displayed every time a user logs onto the system. This banner will reference Federal, State, and DOC regulations, policies, and procedures covering information technology use within the Commonwealth of Virginia.
2. Changes to any messages posted on login banners must have prior approval from either the ISO or the CTO before being implemented.
3. User and account access to DOC systems/network must be identified in accordance with *COV IT Information Security Standard* (SEC 501-06), or by other means providing equal or greater security (e.g. biometric readers, retina scanners etc.), and must be approved by the VITA/NG and CTSU Security groups before accessing any systems/network resources.
4. Server system software will execute with its inherent account as designed by the manufacturer of the software.

### B. Official Use

1. No user should have expectation of privacy when using DOC Information Technology Systems.
  - a. The DOC has the right to monitor all aspects of DOC IT Systems, and such monitoring may occur at anytime, without notice and without the user's permission.
  - b. Monitoring of IT systems and data may include but is not limited to network traffic, application and data access, keystrokes, user commands, email and Internet usage, and message and data content.
  - c. Except for exemptions under the Act, electronic records may be subject to the [Freedom of Information Act \(FOIA\)](#) and therefore, available for public distribution.
2. CTSU Security shall monitor use of all DOC Information Systems for any activity that may be in violation of state and/or DOC policy and procedure. CTSU Security shall review all security settings, configurations, and patch management for security and violations of policy and procedure.
3. *Personal Use of the Computer and the Internet* - Personal use means use that is not job-related. Internet use during work hours should be incidental and limited to not interfere with the performance of the employee's duties or the accomplishment of the unit's responsibilities. Personal use is prohibited if it:
  - a. Adversely affects the efficient operation of the computer system; or



- b. Violates any provision of this operating procedure, any supplemental procedure adopted by the agency supplying the Internet or electronic communication systems, or any other policy, regulation, law, or guideline as set forth by local, State or Federal law. (see [COV §2.2-2827](#))
4. Users of the DOC computer system/network must not use these resources for soliciting business, selling products, or commercial activities other than those expressly permitted by DOC management.
5. The Organization Unit Head will ensure employees, contractors, volunteers and authorized users shall NOT allow offenders to have access (supervised or unsupervised) to any DOC Information Technology Resource connected to the agency's network/systems, or resource that can access the Internet. Any exception must be unequivocally approved by the CTO and Deputy Director.
  - a. **NOTE: Offenders are strictly prohibited from any access to DOC Information Technology Resources on the agency's network/systems or resources that can access the Internet.** Information technology resources not on the agency's network/system or resources that do not have Internet access may be utilized by offenders with written permission from the Regional ~~Administrator~~ ~~Correctional Operations Director~~ (e.g. stand alone devices with office automation software or educational devices intended for offender use).
  - b. **An exception is provided for supervised offenders in the work release program at Virginia Correctional Enterprises with explicit approval of the Deputy Director of Administration.**
  - c. **Offenders shall not have direct and unlimited access to network or local printers. If printing is required, it should be done by DOC staff on an approved device and provided to the offender. (added 2/22/12, added 8/13/12)**
6. No access shall be granted to any DOC Information Technology System, resource, or data by anyone unless said access is granted in accordance with this operating procedure. Based on the scope of work to be performed, a background check is required.
7. Vendors, partners, or other non-DOC entities shall not be granted access to the DOC Information Technology Systems without the express written permission of the CTO. When access is requested, CTSU Security shall provide the CTO with a risk assessment. If access is granted by the CTO to a vendor, partner, or non DOC entity, that entity shall agree in writing to abide by all applicable laws, regulations, and DOC operating procedures prior to receiving access. (see Attachment 3, *IT System Interoperability Security Statement*) (added 2/1/13 per CTO)
8. Posting sensitive data on a public website, ftp server, bulletin board, shared drive or other publicly accessible medium unless a written exception is approved by the Agency Head is prohibited. The exception must include the business case, risks, mitigating controls and all residual risks.
9. When using electronic communication tools and social media, users should follow all applicable Commonwealth policies and be responsible and professional in their activities. Employees should conduct themselves in a manner that supports the mission of the agency and performance of their duties.
  - a. When utilizing social media for business purposes, users should be respectful of the agency, other employees, customers, vendors and others when posting and communicating information. Be aware of any associated potential liabilities and obtain consent prior to communicating or posting information about the workplace.

- b. When utilizing social media for personal use, personal email addresses should be utilized and not those related to their position with DOC when communicating or posting information for personal use.
10. Certain activities are prohibited when using the Internet or electronic communications. These include, but are not limited to:
- a. Accessing, downloading, printing or storing information with sexually explicit content as prohibited by law (see COV §2.2-2827)
  - b. Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images
  - c. Installing or downloading computer software, programs, or executable files contrary to policy
  - d. Uploading or downloading copyrighted materials or proprietary agency information contrary to policy
  - e. Uploading or downloading access-restricted agency information contrary to policy or in violation of agency policy
  - f. Using another employee's DOC network account for any purpose
  - g. Posting information or sending e-mail using another's identity, an assumed name, or anonymously
  - h. Forwarding of joke e-mail, chain letters, personal photographs, etc.
  - i. Forwarding of DOC business data to a personally owned external email address (e.g. Hotmail)
  - j. The use of language, words, or pictures that could be considered offensive to others
  - k. Permitting a non-user to use DOC resources for purposes of communicating the message of some third party individual or organization
  - l. Tampering with security controls configured on COV workstations
  - m. Installing or using proprietary encryption hardware or software on COV systems
  - n. Installing personal software on a COV system
  - o. Adding system hardware to, removing system hardware from or modifying system hardware on a COV system
  - p. Connecting non-COV devices to a COV IT system or network, such as personal computers, laptop, PDA or other handheld device, USB (flash) drives, cell phones and digital music players
  - q. Utilizing a DOC issued laptop device and/or DOC issued mobile phone as one's own personally owned device for personal business.
  - r. Using proprietary agency information, state data records and social media to locate agency customers for personal reasons
  - s. Posting photos, videos or audio recordings taken in the work environment without written consent
  - t. Using agency or organization logos without written consent
  - u. Texting, emailing, or using hand-held electronic devices while operating a state vehicle according to the [Office of Fleet Management Services Policies and Procedures Manual](#)

- v. Streaming audio and video, as it not only slows down the network speed but it also clogs network traffic
- w. Providing application data to individuals who do not otherwise have authorization or access to such information (added 4/30/12)
- x. Any other activities designated as prohibited by the agency

### C. Password Security

1. All DOC password requirements are based on the minimum VITA/NG Standards.
2. All users of DOC IT systems must be identified with a non-generic user-ID and password or by other means that provide equal or greater security. All non-standard methods of access (e.g. biometric readers, retinal scanners etc.) shall be approved by the VITA/NG and CTSU Security before accessing any systems/network resources.
3. Employees must not share accounts or allow others access through their user-ID unless approved by CTSU as a shared account.
4. All accounts will have a password.
5. Passwords must not be displayed on the screen as they are entered.
6. VITA/NG shall implement and maintain the Windows password policy on the Windows Systems once it has been set by CTSU Security.
7. Passwords must be implemented on mobile devices issued by DOC (Blackberry, iPhone, PDA, etc.) The password requirement is a minimum of 4 characters. (added 4/30/12)
8. Windows passwords must be at least 9 characters and are case sensitive. Open VMS passwords are between 8 and 15 characters and are not case sensitive.
9. All users should choose passwords, with a combination of at least three of the following types of characters.
  - a. Alpha Characters (a-z)
  - b. Numeric Characters (0-9)
  - c. Capitalized Characters (A-Z)
  - d. Symbols and Punctuations (#!\$%^&\*)
  - e. Examples of how to pick a strong password without making it too complex to remember
    - i. Take two words like “two sticks” and capitalize some letters and substitute symbols and numbers.
    - ii. two sticks = Tw0\$t1cK\$ This password has alpha characters, numeric characters, and punctuation or symbols so it meets the requirements.

*Note: DO NOT USE THIS EXAMPLE AS YOUR PASSWORD! THIS IS ONLY AN EXAMPLE!*
10. The password must NOT be related to the user’s job or personal life or a word found in the dictionary as most common words can be easily ‘cracked’ by a password cracking tool.
11. The system will prompt users to change their passwords every 90 days. A password may not be reused that was used in the previous 24 changes.
12. After four unsuccessful attempts to enter a password, the user-ID involved will be:

- a. Temporarily disabled
- b. Once a password is locked out, users must contact the VCCC to have the password unlocked

~~13. Windows and Open VMS password related requests for assistance (e.g. forgotten passwords, locked accounts, logon id suspensions) shall be submitted to CTSU Security the VCCC. (deleted 5/15/12)~~

14. Anyone that installs any device or software on DOC systems will change all default passwords on all devices, service accounts, or software before it is used by DOC employees. This refers to all vendor default passwords on ALL devices or software packages. Passwords shall not appear as plain text in any scripts.
15. Passwords should not be written down or left in a place where unauthorized persons might discover them. (e.g. under keyboard, top drawer of desk, under mouse pad, taped to PC).
16. If any user suspects that his/her password may have been disclosed, he/she must immediately change the password or notify the ISO or CTSU Security.

#### D. Logging Off, Locking, and Rebooting Workstations

1. All workstations, when unattended even for short periods must be locked and password protected. The locking screen saver on all PCs has been set to take effect within 30 minutes if there is no activity on the workstation. Devices with access to sensitive systems or those devices in less physically secure environments must have a lower time-out interval documented and enforced, in accordance with *COV ITRM Standard SEC 501-06*.
2. When users have completed work for the day, they should put their workstation in stand-by mode. Shared workstations must either log off or reboot their workstations. Due to the need to patch software, update virus definitions, or perform other maintenance on PCs after hours, a complete shutdown is not required unless CTSU requests it.
3. All servers must be configured with the screen saver settings to take effect within 2 minutes and lock the server if there is no activity on the server.
4. Users should reboot their PCs at least weekly to ensure PC health and that security patches and updates that have been applied take effect.

#### E. Internet Services Usage

1. DOC Internet Sites and Visitor Privacy
  - a. The DOC uses VIPNet to host state web sites. To function properly, some VIPNet applications create “cookies” containing information found on users’ computers. The applications place those “cookies” on the computers and notify users of their creation.
  - b. The DOC Public Internet site does not:
    - i. Record personal information of visitors
    - ii. Record movements of visitors through the site
    - iii. Record dates and times of visits
    - iv. Record Internet browser information
  - c. DOC reserves the right to modify Internet privacy policy and procedures at any time and without prior notice.
2. Filtering, Monitoring, and Inspection

- a. The CTSU Security Office filters, monitors, and inspects activities and information related to the use of DOC Systems and Internet services to ensure these services are used only for acceptable, appropriate, and authorized purposes. CTSU Security blocks access to known pornographic, gambling, and other unacceptable, inappropriate, and unauthorized web sites.
  - b. An employee is notified of any attempted visit to an inappropriate and unauthorized web site, whether intentional or not, by a warning message. The employee should notify his supervisor when he receives a warning message.
  - c. An employee must notify his supervisor and CTSU Security (via the CTSU Security Mailbox: ([CTSUSecurity@vadoc.virginia.gov](mailto:CTSUSecurity@vadoc.virginia.gov))) if he gains access to a pornographic, gambling or other web site designated by the DOC as inappropriate and unauthorized, whether intentional or not.
  - d. Unacceptable, inappropriate, and unauthorized use of Internet services will be investigated and acted on in accordance with *Employee Standards of Conduct*, (see Operating Procedure 135.1).
  - e. If an employee has visited or attempted to visit one or more unauthorized web sites the following procedure will be followed.
    - i. CTSU Security will deliver a written report of the employee's activity to the employee's organizational Unit Head.
    - ii. CTSU Security will deliver copies of the report to Human Resources, the Inspector General and the CTO.
    - iii. The organizational Unit Head will give notice of the report to the employee, the employee's Supervisor, and to the Unit Head's supervisor (i.e. **Chief of Corrections Operations** ~~Deputy Director of Operations~~, Deputy Director of Administration, ~~Deputy Director of Community Corrections~~, Regional **Administrators** ~~Directors~~, or Inspector General).
    - iv. The Unit Head may request the employee's access to the Internet be suspended. Access may be reinstated only if requested by the Unit Head.
    - v. If a supervisor reasonably suspects that an employee has intentionally visited or attempted to visit one or more unauthorized web sites, the supervisor, through the Organizational Unit Head, will request CTSU Security to analyze the Internet activity of the employee.
3. Acceptable, Appropriate, and Authorized Usage
- a. DOC Internet services support job functions, communications, information exchange, and collaborative work.
  - b. All Commonwealth of Virginia and DOC policies and procedures regarding conduct of personnel relevant to the use of Internet services apply to the use of those services.
  - c. DOC authorizes only legal and ethical use of Internet services.
  - d. DOC requires users of Internet services to respect copyrights, software licensing rules, property rights, and the privacy and prerogatives of others.
  - e. Utilization of USB (flash) drives must only include those that are encrypted
  - f. Use of Internet services is a privilege that can be revoked.
  - g. Specific acceptable, appropriate, and authorized usages of Internet services include, but are not limited to, activities supporting:

- i. Job functions, communications, information exchange, and collaborative work directly related to the charter, mission, goals, and purposes of the DOC
  - ii. Applications for, and administration of, grants and contracts for DOC research projects or other programs
  - iii. Dissemination or distribution of laws, policies, procedures, rules, programs, services, activities, or other official information
  - iv. Administrative communications not requiring a high level of security
  - v. Employees' pursuit or maintenance of training, education, or certifications related to their job function and responsibilities.
  - vi. Professional society activities related to employees' job responsibilities and activities
  - vii. Administrative communications and discussions related to employees' job responsibilities and activities
- h. If business need requires access to blocked content, access may be requested by the user's Unit Head via the CTSU Security Mailbox: ([CTSUSecurity@vadoc.virginia.gov](mailto:CTSUSecurity@vadoc.virginia.gov))
4. Unacceptable, Inappropriate, and Unauthorized Usage
- a. DOC has no tolerance for employees, contractors and volunteers who use DOC Internet services and information technology (personal computers, networks, etc.) for unacceptable, inappropriate, and unauthorized purposes.
  - b. If the DOC determines that an employee, contractor, or volunteer has visited or attempted to visit one or more pornographic, gambling, or other web sites designated by the DOC as unacceptable, inappropriate and unauthorized, the employee, contractor, or volunteer shall be reported to their organizational unit head for appropriate action under Operating Procedure 135.1, *Employee Standards of Conduct*.
  - c. Specific unacceptable, inappropriate, and unauthorized usages of Internet services include, but are not limited to:
    - i. Violations of federal or state laws or violations of state or DOC policies or procedures
    - ii. For-profit activities, excluding those directly related to the DOC's charter, mission, goals and purposes, or employees' job responsibilities and activities.
    - iii. Private business, including commercial advertising
    - iv. Personal or other non-DOC related fund raising or public relations activities, excluding those approved by the Director or the Director's designee
    - v. Intentional modification of passwords, files, or other data belonging to another employee without prior approval from either the employee or their supervisor
    - vi. Creation, transmission, retrieval, or storage of material or messages of a libelous, defamatory, derogatory, inflammatory, discriminatory, or harassing nature, including, but not limited to, those relating to race, ethnicity, national origin, religion, political affiliation, gender, and age, or physical, mental, and emotional disability
    - vii. Access, use or distribution of computer games that are unrelated to the DOC's, mission, goals and purposes, or employees' job responsibilities and activities, but excluding computer games that teach, simulate, or illustrate DOC-related information and activities which are approved by management and then installed by an LSA.
    - viii. Interference with information technology users, services, or equipment including, but not limited to, those usages developing or propagating malicious code, attempting unauthorized access to another employee's computer, distributing advertisements, or sending chain mail

- ix. Using the network to gain unauthorized entry to another machine on the network
- x. Storing of music files or personal photographs on the DOC network LAN
- xi. Utilizing an external account (e.g. Hotmail, Yahoo) to conduct official DOC business
- xii. Allowing access to the Internet, DOC network, LAN, WAN or other network to any person who has not received access approval from the DOC
- xiii. Placing obscene material on the DOC computer network, for use, access, or distribution of sexually explicit, indecent, or obscene material

#### 5. Pornography

- a. The use of DOC Internet services or any DOC Information Technology System for visiting pornographic web sites, or for accessing, storing, or distributing pornographic material, is prohibited.
- b. CTSU will monitor DOC employees', DOC Contractors', and volunteers' Internet access for hits and blocks on pornographic, gambling, and other inappropriate websites. CTSU Security will report violations of this operating procedure to the violator's Organization Unit Head.
- c. DOC employees, contractors, and volunteers are strongly encouraged to review all [Code of Virginia](#) sections and [United States Code](#) sections related to information technology.
- d. The following laws, standards, and guidelines govern the use of Commonwealth of Virginia and DOC Information Technology, including Internet services, with respect to pornographic web sites and materials, and other unacceptable, inappropriate, and unauthorized web sites and materials, by Commonwealth and DOC employees, contractors and volunteers. Users of DOC Systems must adhere to these procedures, codes, and laws while using DOC Systems.
  - i. Operating Procedure 135.1, *Employee Standards of Conduct*
  - ii. [COV §18.2-374](#) states, in part, that possession, production, reproduction, publication, distribution, transportation or sale of obscene items is unlawful.
  - iii. [COV §18.2-372](#) Definition of Obscenity
  - iv. [18 United States Code Section 1465](#) states, in part, that interstate transportation or communication, via computer or other means, of obscene materials is unlawful. Any person found in violation of this code shall be fined or imprisoned, or both.
  - v. [COV §2.2-2827](#), defines restrictions on state employees' access to any information infrastructure. DOC shall immediately furnish current employees with copies of this code section's provisions, and shall furnish all new employees copies of this section concurrent with authorizing them to use agency computers.
  - vi. [COV §18.2-374.1:1](#) defines possession of child pornography and describes the legal penalty for such acts. All sexually explicit visual material which utilizes or has as a subject a person less than 18 years of age shall be subject to lawful seizure and forfeiture pursuant to [§18.2-374.2](#).

#### F. E-Mail Usage

- 1. The DOC e-mail system, and all e-mail accounts and their associated messages and attached files, are the property of the Commonwealth of Virginia and should be used for appropriate business purposes.
  - a. Appropriate use refers to job functions, job communications, information exchange and collaborative work directly related to the mission, goals and business of the Department.

- b. Personal, non-work related or inappropriate comments, graphics, quotes, links or other non-business related items are not permitted in official communications, using email or other media.
2. Back-up copies of e-mail messages and attached files may be stored and referenced for operational and legal purposes. Contents of e-mail messages and files may be disclosed without employees' permission, to appropriate and authorized DOC personnel and to law enforcement officials.
3. The DOC e-mail systems, and all e-mail accounts and their associated messages and attached files are subject to monitoring by CTSU Security to ensure adherence to all relevant DOC policies and procedure, Virginia codes and laws, and United States codes and laws. This monitoring can occur at any time without the user's consent or notification.
4. E-mail shall not be used to send sensitive data unless encryption is used. The transmission of e-mail and attached data that is sensitive relative to confidentiality or integrity is required to be encrypted; however digital signatures may be utilized for data that is sensitive relative to integrity.
5. E-mail at DOC is subject to all the terms and conditions in Section E., above, *Internet Service Usage* in this operating procedure.
6. Any user of the DOC network who receives an e-mail message violating the *Internet Service Usage* requirements, stated in Section E., above, should report the incident to their immediate supervisor. The supervisor should then contact CTSU Security.
7. DOC e-mail must not be auto-forwarded to an external e-mail address unless there is a documented business case provided to CTSU Security by the Unit Head.
8. E-mails may often be used in legal or other administrative proceedings that were not anticipated when the message was sent. Freedom of Information Act requests, court subpoenas, or other unexpected situations can place an electronic message in front of someone that you did not anticipate. An electronic message is just as "official" as a letter typed on letterhead stationery and mailed to the recipient through the postal service. Personal or inappropriate comments, graphics, quotes, links, or other non-business related items cannot be included in official communications, electronic or otherwise.
9. Standard framework for electronic message "auto signatures".
  - a. Users are authorized to give their name, job title, agency, address, phone numbers, and e-mail address when creating messages and replying to others. For example:
 

John Doe, Bureau Chief  
Virginia Department of Corrections  
P.O. Box 26963  
6900 Atmore Drive  
Richmond, Virginia 23261-6963  
Telephone 804-674-3000  
Fax 804-674-3001  
E-mail John.Doe@vadoc.virginia.gov
  - b. No other non-business related graphics, quotes, links, etc. are allowed in "auto signature". This does not include a simple graphic or personal comment used in a clearly personal message sent to a single user.

#### G. Virus Suppression



1. All DOC employees are required to exercise caution when opening files retrieved from the Internet or received via electronic mail.
2. Files that have been downloaded or received should be subject to the virus checking software provided by DOC before those files are opened or executed.
3. VITA/NG is responsible for supporting and maintaining the agency's anti-virus enterprise software and ensuring that current definitions and updates are pushed out to the network/system.
4. Each organizational unit will be responsible for contacting **CTSU Security** ~~the VCCC~~ to provide assistance in correcting any damage to a desktop personal computer if it becomes infected with a virus. (changed 4/30/12)
5. All PCs/workstations in use within DOC must have VITA/NG approved virus suppression software, with the latest release, loaded and activated on their PC/Workstation.
6. DOC users are prohibited from intentionally developing, deploying, using, or experimenting with malicious programs, including but not limited to viruses, adware, worms, spyware, Trojans, and keystroke loggers.

#### H. Security Incident Reporting

1. An IT security incident refers to an adverse event in an information system, network, and/or workstation, or the threat of the occurrence of such an event. IT security incidents must be immediately reported to the ISO by e-mailing [CTSUSecurity@vadoc.virginia.gov](mailto:CTSUSecurity@vadoc.virginia.gov). If e-mail is known or suspected to be compromised, report the incident through alternate channels that have not been compromised. In addition, the incident must be reported by telephone to the ISO or CTO.
2. Document and report details that may be of relevance including date, time, name(s), location(s), systems, networks, and other significant information. To preserve evidence, no action beyond immediate notification to CTSU Security should be taken by any individual without the express direction of the CTSU Security Office.
3. All IT security incidents should be reported to CTSU Security using the [IT Security Incident Report](#) 310\_F6. All report information must be e-mailed to the CTSU Security Office ([CTSUSecurity@vadoc.virginia.gov](mailto:CTSUSecurity@vadoc.virginia.gov)) and followed up by mailing a hard copy of the *IT Security Incident Report* to the following address:
  - Corrections Technology Services Unit
  - CTSU Security Group
  - P.O. Box 26963
  - Richmond, Virginia 23261-6963
4. The ISO must report IT Security incidents to the COV CISO and to the Information Systems Auditor in the DOC Internal Audit Unit within 24 hours of receiving notification.
5. The following are examples of IT security incidents:
  - a. System impairment due to improper usage / denial of service
  - b. Unauthorized access or repeated attempts at unauthorized access from either internal or external sources
  - c. Virus attacks which adversely affect servers or workstations
  - d. Theft, loss, or vandalism of DOC software or hardware

- e. Web site defacement
  - f. Intrusion or intrusion attempts into unauthorized system or user accounts
  - g. Unauthorized access, use, disclosure, alteration, manipulation, destruction or other misuse of DOC data
  - h. Circumvention of IT security controls, safeguards or procedures
  - i. Inappropriate use of the internet or electronic e-mail as defined in this operating procedure
  - j. Connecting to or tampering with another users PC without written authorization
  - k. Installing hardware or software that has not been approved by CTSU
  - l. Accessing or attempting to access, copy, read, or manipulate data in any way that is not owned by the person attempting access, directly related to their job description, or for which the person attempting access has no legitimate right or need to access the information.
  - m. Unauthorized release of unencrypted sensitive information (data breach) that is not otherwise obtainable from publicly available resources, or from federal, state or local government records lawfully made available to the general public. This information includes first name (or initial) and last name in combination with and linked to any one or more of the following data elements *that relate to a resident of the Commonwealth*, when the data elements are neither encrypted nor redacted:
    - i. Social security number (at least 5 digits);
    - ii. Drivers license number or state identification number (at least 4 digits); or
    - iii. Financial account number, or credit card or debit card number, in combination with any required security code, access code or password that would permit access to a resident's financial accounts
    - iv. Any information regarding an individual's medical or mental health history, mental or physical condition or medical treatment or diagnosis by a health care professional
6. If after CTSU Security investigates the reported security incident and determines that the incident needs further investigation, CTSU Security should notify the Office of Inspector General to perform a more thorough investigation of the incident.
- I. **Criminal History Information, Procedure, and Responsibilities (VCIN) (added 2/22/12)**
- 1. Criminal history information requested by someone other than the authorized VCIN operator will be personally presented to the requester or sent in a sealed envelope marked "CONFIDENTIAL"
  - 2. A criminal history record shall not be given to non-criminal justice agencies and shall not be disseminated by radio or telephone except in an urgent or emergency situation, or for purposes of staff safety.
  - 3. A record of all criminal history requests will be maintained in a *Criminal History Request Log* as specified in the VCIN manual.
  - 4. When criminal history records have served the purpose for which they are intended, they shall be destroyed by burning or shredding.
  - 5. There will be no unauthorized access or dissemination of any information obtained from VCIN. Violations will be handled in accordance with the Code of Virginia and Operating Procedure 135.1, *Standards of Conduct*.

J. Telephone Usage (added 2/22/12)

1. Personal Calls

- a. Local personal calls which have to be made during working hours may be made from DOC telephones, but their number and duration shall be kept to a minimum.
  - b. Long distance personal calls shall not be made from DOC telephones unless charges are reversed or charged to the employee's personal telephone number or personal credit card account.
2. Employees shall not access 900 numbers or any other number which constitutes a charge to the Commonwealth.
  3. Organizational Unit Heads will be responsible for monitoring usage of DOC telephones and reviewing any billing statements to detect inappropriate usage.

VII. INFORMATION TECHNOLOGY SYSTEM MANAGEMENT

A. Software Authorization

1. Special technical software and hardware specifications for special units within DOC shall be maintained with those unit's inventories and auditing documentation. No Information Technology Initiative shall commence without prior written notification and approval of the CTO of CTSU.
  - a. The CTO will make appropriate CTSU staff assignments (if needed) within two weeks of receipt of the request.
  - b. No software for use by more than one user shall be bought, downloaded, developed, programmed, or installed on the DOC network without express written approval from the CTO.
    - i. The CTO must approve software use that falls outside of the DOC standard configuration. A written request to the CTO must be sent through the requesting employee's supervisor.
    - ii. Requests for software to be installed must be submitted to CTSU Security. If not obvious, an explanation of the use for the software is required. Proof of license is also required. (added 4/30/12)
2. Sensitive data shall not be used or stored in non-production environments (i.e., a development or test environment must have security controls equivalent to the production environment.)
3. VITA/NG and CTSU Security reserve the right to refuse all software that it considers to be Malware or hacking tools. Any request that is accepted or rejected will be forwarded to CTSU Security ([CTSUSecurity@vadoc.virginia.gov](mailto:CTSUSecurity@vadoc.virginia.gov)) for follow up with the requestor.
4. DOC is a member of the Microsoft Select and Enterprise Agreement. Membership in this agreement allows DOC to acquire Microsoft Licensing for operating systems and office automation products. Procedures located on DOCNET shall be followed when users wish to obtain, procure, and use the products. A hard copy of this operating procedure may be requested through e-mail to the CTSU Fiscal Administration and Security group.
5. Employees and contractors shall NOT allow offenders access (supervised or unsupervised) to software applications that are not stand-alone.
  - a. Workstations in facilities accessible by offenders must be located in offices or enclosed areas which can be locked and secured.

- b. Offenders shall not have direct and unlimited access to network or local printers. If printing is required, it should be done by DOC staff on an approved device and provided to the offender. (added 2/22/12, 8/28/12)
  - c. Any exception must be unequivocally approved by the CTO and Deputy Director.
6. All standalone workstations that have been formerly used by offenders must be reformatted and their operating systems and software reinstalled by contacting **CTSU Security** ~~the VCCC~~ **and opening a ticket** prior to attaching the workstation on the DOC network. (changed 4/30/12)
  7. Users who have to access both their PC and offender standalone workstations must write-protect any floppy disks exchanged between networked and offender used machines to avoid infestation of their floppy with possible viruses or malware.
  8. All files on floppy disks, CD's, flash drives, and tapes must be scanned with anti-virus software prior to writing data to their PC or network if they have been used on offender PCs or have been used outside of the DOC.
  9. The installation of software products that the software publisher has designated as end-of-life (i.e. the software publisher no longer provides security patches for the product) is prohibited.
  10. Employees and contractors shall NOT allow unauthorized individuals access to DOC equipment or DOC software applications used for official purposes.
  11. VITA/NG is responsible for all security patches, hot fixes, and updates for software on DOC IT Systems. Unless otherwise authorized, users are not permitted to download and apply updates to any software.
  12. DOC users are encouraged to save data to their W drive (network share) rather than their computer hard drive (C:\) due to the fact that computers could potentially crash or become infected and a user may lose data. (added 11/2/12)

#### B. Hardware Authorization

1. No Information Technology hardware shall be installed, used on, or connected to DOC IT Systems by non-CTSU staff without prior knowledge or approval from VITA/NG and CTSU Security. Examples include but are not limited to routers, switches, hubs, servers, workstations, wireless IT equipment, PDAs, removable drives and storage, printers, or any other Information Technology device or peripheral.
2. Requests for hardware to be connected to the network should be sent to the VCCC.
3. New and replacement DOC workstations/PCs are leased from the Virginia Information Technologies Agency (VITA). Current specifications and prices can be obtained from the [VITA web site](#). Workstations that require reloading or configuring will be returned to the approved image when purchased or otherwise noted by VITA/NG.
4. Only DOC approved mobile data storage devices may be used on, or connected to DOC IT Systems. USB devices (e.g. flash drives) utilized within DOC must be encrypted.
5. Vendors, contractors, or any other non-DOC personnel who need to connect IT hardware to the DOC Systems must have written approval of CTSU Security and be provided a copy of this operating procedure. Any IT hardware attached to DOC IT Systems will be subject to this operating procedure.
6. All hardware systems connected to the DOC Network must utilize appropriate virus protection software and maintain up-to-date virus definitions and will be subject to security scans and

should have no expectation of privacy.

7. All IT hardware connected to DOC IT Systems should be up to date with all applicable hot fixes and or security patches.
8. Any vendors, contractors, or non-DOC personnel that do not meet this requirement or do not agree to this operating procedure should not connect any devices to the DOC Systems or Network.

#### C. Wireless Equipment Security

1. Wireless IT equipment has unique security risks and should not be employed within DOC without the written consent of CTSU Security, CTSU Operations, and the VITA/NG Network group. Requests for wireless equipment should be sent to ~~CTSU Security the VCCC who will notify CTSU Security staff.~~ (changed 4/30/12)
2. Any wireless IT equipment deployed within DOC will be evaluated on a case-by-case basis and may have different requirements based on its requested location and use. CISCO is the standardized wireless equipment utilized within the DOC.
3. Wireless IT equipment is subject to monitoring and scanning by CTSU Security at any time without notification or consent and is subject to all aspects of Section VI., E., *Internet Services Usage*, and Section B., above, *Hardware Authorization*.
4. All wireless equipment attached to COV DOC IT systems must run 128 bit or greater encryption and be able to successfully pass a wireless security scan by CTSU Security.
5. DOC workstations may be connected to trusted wireless networks, which are those networks utilizing a secure encryption protocol such as WPA (WEP is not considered secure), and those managed by another COV agency. DOC workstations may NOT be connected to untrusted wireless networks.
6. DOC devices ~~remotely~~ connecting to the WLAN must utilize two factor authentication. ~~(i.e., digital certificates.)~~ (changed 9/26/13)
7. Unauthenticated internet access is not permitted on DOCs WLAN.
8. Wireless access points (AP) are limited to authorized domain users with properly configured wireless clients.
  - a. ~~A Wireless Guest Network has been established for the purpose of providing controlled access to the Internet for users without a Commonwealth of Virginia network account~~
  - b. ~~Each facility designates a Wireless Guest Network administrator(s).~~
  - c. ~~Wireless Guest Network privileges will not be assigned to personal mobile devices (iPhones, iPads, etc.).~~
  - d. ~~Wireless Guest Network accounts must not be shared.~~
  - e. ~~Wireless Guest Network accounts should only be granted for the time period required in order to conduct official DOC business. If an extended time period is required, an exception from CTSU Security should be requested.~~ (added 9/26/13)
9. Only COV owned or leased equipment shall be granted access to an internal WLAN.
10. Physical or logical separation between the WLAN and wired LAN segments must exist.

#### D. Encryption and Data Security

1. Encryption adds an additional layer of security and the CTSU Security Office recommends that it be used whenever possible to protect sensitive or confidential data.
2. All internal IT communications should be encrypted whenever possible.
3. All external IT communications transmitted via e-mail should be considered sensitive. Users are reminded to consider data that should not be shared externally prior to transmitting.
4. Any new processes, protocols, or applications that pass credentials in clear text cannot be used internally and MUST NOT be used externally. (examples – FTP, TELNET) Existing processes using these technologies must be remedied as soon as possible.
5. All encryption should be 128 bit or greater.
6. Sensitive documents printed to a globally shared printer should be retrieved immediately.
7. When no longer needed, shred documents and erase white or blackboards of sensitive data.
8. Electronic records should be retained in accordance with the retention requirements of the Library of Virginia

E. Security Awareness Training

1. The Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Standard SEC501-06 requires that all state agencies establish and maintain an IT security awareness program to ensure that all individuals are aware of their security responsibilities and know how to fulfill them.
  2. It is the responsibility of the Organizational Unit Heads to ensure all employees assigned a DOC IT Systems account participate in the required IT Security Awareness Training (SAT) annually. (4-4101)
  3. All new employees should take IT Security Awareness Training within thirty days of receiving access to DOC IT Systems.
  4. If extenuating circumstances such as extended annual leave, extended sick leave, short-term disability, military leave, etc. prevent a user from meeting a required due date, the user must complete IT Security Awareness Training within thirty days of their return to work.
  5. Employees taking the IT Security Awareness Training MUST utilize their DOC Windows account; failure to logon using the correct account will result in not receiving credit for the training.
  6. Employees, excluding those on extended leave, failing to complete the training will be in violation of Operating Procedure 135.1, *Employee Standards of Conduct*, and may be subject to disciplinary action.
  7. Employees taking IT Security Awareness Training are required to read the DOC Information Security Agreement contained in the training. By completing the training, the employee acknowledges that he or she agrees with all stipulations in the Security Agreement and will abide by the agreement. Failure to abide by the agreement will be a violation of Operating Procedure 135.1, *Employee Standards of Conduct*, and the employee may be subject to disciplinary action and will result in non-completion of training.
- F. Removal of Data from Hardware (including copiers), Data Storage Devices, and Media - Prior to its being surplus, transferred, traded-in, disposed of, or replaced, Department of Corrections data shall be removed from all electronic media resources in accordance with *Removal of*

*Commonwealth Data from Electronic Media (SEC514-03).*

VIII. REFERENCES

[18 United States Code, Crimes and Criminal Procedure, Section 1465](#)

COV ITRM Standard SEC501-06, *IT Information Security Standard (SEC501-06)*

COV ITRM Standard SEC514-03, *Removal of Commonwealth Data from Electronic Media (SEC514-03)*

Deputy Director Memo 2/22/05, Electronic Messaging

[DHRM Policy #1.75 Use of Internet and Electronic Communications Systems](#)

Operating Procedure 135.1, *Employee Standards of Conduct*

[Office of Fleet Management Services Policies and Procedures Manual](#)

IX. FORM CITATIONS

[Windows Admin/System Security Agreement](#) 310\_F1

[Windows/VMS User Account Request](#) 310\_F2

[Windows/VMS User Information Security Agreement](#) 310\_F3

[Windows Admin/System Account Request](#) 310\_F4

~~[Remote Access to DOC Applications and IT Resources](#) 310\_F5 (deleted 11/2/12)~~

[IT Security Incident Report](#) 310\_F6

X. REVIEW DATE

The office of primary responsibility shall review this operating procedure annually and re-write it no later than October 1, 2014.

*The office of primary responsibility reviewed this operating procedure in October 2012 and necessary changes have been made.*

## Signature Copy on File

---

N. H. Scott, Deputy Director of Administration

## **ATTACHMENT H**

### **SERVICE LEVELS**

Kiosk and network issues are resolved within the following timeframe: between 4 hours and 4 business days. Resolution may take 4 days or longer if the issue is considered an exception, i.e. we are waiting on an order for spare parts, we need to repair damaged fiber, clearance delays, escort issues, etc. Some issues require VADOC assistance, such as power and network failures.

Issue reporting, communications, and resolutions are handled by JPay's Help Desk Team, Field Engineering Team, and NOC (Network Operation Center).

The Help Desk is responsible for technician clearances, scheduling, assistance with mailroom PC's, inquiries from Investigators, Trust Accountants, and other staff. Help Desk also resolves issues with the Offender Management System for file transfers and all such file issues are intended to be resolved within 24 hours.

Onsite Field Engineers are deployed to resolve hardware, network, and power issues. For all onsite calls, our goal is to have someone on site within 24 hours of the issue being identified and reported. As it is not always possible to have someone onsite within 24 hours, we aim to have someone onsite no later than 4 business days not including the exceptions described above.

The NOC detects prolonged downtime by watching the network and the frequency of offender logins. The NOC performs remote reboots to resolve the vast majority of kiosk outages on the same day that they're



reported. If an issue is not detected by the NOC, it is most likely detected in the offender support tickets and in the direct communication from the VADOC staff via email and phone and resolved within 72 hours.

## **ATTACHMENT I**

### **BENCHMARKS**

- 1) JPay shall provide satisfactory customer service to the VADOC as documented on the Contractor Evaluation Report (See Attachment J.). 80% of the participating institutions must report an overall satisfactory report. A 4 and 5 rating will be considered satisfactory on the Performance Evaluation.
- 2) JPay shall deliver players with a 90% success rate, meaning a minimum of 90% of all players will function perfectly upon arrival.
- 3) JPay shall keep the song catalog updated in real time throughout the term of the pilot.
- 4) All kiosks will be functional or repaired within 72 hours of a service call being placed, excluding holidays.

**ATTACHMENT J**

**CONTRACTOR PERFORMANCE EVALUATION REPORT**

Contract Number: \_\_\_\_\_

Contractor: \_\_\_\_\_

Evaluator/Administrator: \_\_\_\_\_

Date Submitted: \_\_\_\_\_

Period of Evaluation: From: \_\_\_\_\_ To: \_\_\_\_\_

**RATE CONTRACTOR'S PERFORMANCE ON A SCALE OF 1 TO 5 (by circling)**

- |    |                         |   |   |   |   |   |              |
|----|-------------------------|---|---|---|---|---|--------------|
| 1. | Overall Evaluation      |   |   |   |   |   |              |
|    | Unsatisfactory          | 1 | 2 | 3 | 4 | 5 | Satisfactory |
| 2. | Delivery Performance    |   |   |   |   |   |              |
|    | Late/Early (if problem) | 1 | 2 | 3 | 4 | 5 | On Time      |

3. Quality of Goods/Services
- |              |   |   |   |   |   |            |
|--------------|---|---|---|---|---|------------|
| Unacceptable | 1 | 2 | 3 | 4 | 5 | Acceptable |
|--------------|---|---|---|---|---|------------|
4. Number of Complaints
- |      |   |   |   |   |   |     |
|------|---|---|---|---|---|-----|
| High | 1 | 2 | 3 | 4 | 5 | Low |
|------|---|---|---|---|---|-----|
- Explain any complaints below.
5. Contractor's Responsiveness to requests to correct deficiencies:
- |               |   |   |   |   |   |                                |
|---------------|---|---|---|---|---|--------------------------------|
| Nonresponsive | 1 | 2 | 3 | 4 | 5 | Takes prompt corrective action |
|---------------|---|---|---|---|---|--------------------------------|
6. Renew this contract?
- YES\_\_\_ NO\_\_\_ If No, Please explain in comments below.

Note: Any score of 3 or less must be described in detail below as to what action was taken to remedy the contractor's poor performance and what steps the contractor took to correct the deficiency cited. (Continue on separate sheet if necessary.)

7. COMMENTS: \_\_\_\_\_