Department of Corrections
Memorandum of Understanding
Contract Number DOC-13-040

The Virginia Department of Corrections ("DOC" or "Purchasing Agency") and JPay, Inc. ("Contractor") have agreed to the following:

A. GENERAL:

Electronic Lock Box services will enable family, friends and relatives of DOC offenders to send money electronically to offender trust accounts. Prior to this agreement the DOC allowed multiple vendors to provide this service. Attaining a sole provider will help to eliminate the current administrative burdens that are the result of processing money orders internally at the various DOC facilities.

B. SECURITY REQUIREMENTS:

1. The Contractor shall adhere to all DOC security requirements. See Attachment III "Security Requirements" of this Memorandum of Understanding for the 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 IV "Information Technology Security".

C. CONTRACTOR RESPONSIBILITIES:

The Contractor shall:

1. Receive the funds from the sender in accordance with its collection methods (this would include phone, internet, walk-in and money orders). This shall be done at no cost to the DOC or the offender population.

2. Provide an electronic file of the previous day's transaction activity. This daily file will be available for DOC use by 1 am EST each day. Detailed requirements for the daily file are to be determined by the VirginiaCORIS software provider for the DOC. The electronic file will also include information on funds received by mail from money orders as described under the Lockbox section below.

3. Use the offender file provided by the DOC so that funds are accepted only for valid offender names and offender numbers. Detailed specifications for the offender file are to be determined by the software provider of VirginiaCORIS, similar to that currently in production with all current vendors.

4. Guarantee delivery of funds after the electronic file of daily transactions is made available to the DOC. In instances of fraudulent or erroneous transactions, the DOC may try to assist in recovery if the funds are still in the offender's account.

5. Deposit collected funds (including money orders) via Automated Clearing House (ACH) every weekday (once per day) for the previous day's transactions. For example, transactions received on the weekend will be aggregated in the Monday electronic file of daily transactions and deposited via ACH on Tuesday. In the case of State holidays, processing will be delayed until the next business day. This is necessary for accounting staff to balance daily batches and make sure funds are posted properly.

6. Store details of all transactions in a database and make each transaction available to DOC via an online interface provided by the Contractor. This interface will allow DOC to look up transactions and provide an intelligence feature that allows DOC to see who is sending money. The user interface shall be able to show links between senders and offenders, how many offender are receiving funds from a particular sender, and

how many offenders are receiving funds from multiple senders. The transaction database shall include transactions with other prison systems serviced by the Contractor to the extent possible through data sharing agreements.

7. Allow all transactions to remain available to the DOC for review, whether via the online interface or an archive retrieval process, according to State of Virginia records retention standards.

8. Respond to and resolve any inquiries and complaints from senders arising out of the Contractor's failure to timely transmit any transactions to the DOC.

9. Keep all information about offenders confidential and make no disclosure to any third party, except as required by law. The Contractor shall give the DOC immediate notice of any such disclosure.

10. Submit to the DOC for review and approval any advertisement or promotional material referring to the Commonwealth or State of Virginia or DOC and/or the operation or existence of this electronic funds system.

11. Provide a secure system so that unauthorized users cannot access DOC's information.

Requirements specific to the Lockbox:

The Contractor shall:

1. Provide a lockbox service for money orders received for offenders housed at DOC facilities. This would include processing money orders received daily and combining transactions with the electronic funds file transmittal described above.

2. Design a form document (see item #12 below) and make it available at DOC facilities and over the internet. An electronic copy will also be available on the DOC public website.

3. Collect sender first name, last name, address and phone number for every money order.

4. Provide functionality to allow DOC to control and restrict the flow of funds to and from various individuals.

5. Provide 24/7 customer service, via email and a toll free phone number, which must be available for offender families to inquire about their money orders. Contractor shall put forth best efforts to resolve email inquiries within one (1) to two (2) business days after receipt of the email; the Contractor shall put forth best efforts to resolve phone inquiries during the call, with 90% of all call inquiries resolved before the customer hangs up the phone.

6. Provide a five day turnaround for money orders so that they are available for offenders to spend a maximum of five days after the sender has placed the money order in the mail to the Contractor. Maintain a five day turnaround for money orders that are sent from any state in the US.

7. Maintain a five day turnaround for money orders even if the lockbox operation is located outside of the State of Virginia.

8. Accept money orders from retail locations (i.e. "walk-in) and have a relationship with the major retail locations within the State of Virginia as well as surrounding states.

9. Require money order senders to fill out a form with their address and phone number to be submitted together with the money order. The Contractor can collect more information on this form if it will increase intelligence gathering.

10. Provide a secure lockbox at each facility. It must have at minimum restricted facility access, security and an alarm system, at a minimum.

11. Maintain infrastructure security, meaning that all of the Contractor's software must have formalized change management control, full system redundancy, and capacity for unexpected growth.

12. Require Contractor staff considered to be "lockbox personnel" to undergo DOC background checks. The DOC reserves the right to review and approve the results upon request.

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. WARRANTY:

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

F. FEES

Fees for services will be outlined in Attachment V, "Inmate Banking Fees".

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.virgnia.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. All necessary repairs or corrections shall be completed within 48 hours of the initial notification.

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 successive one year periods, under the terms of the current contract, and at a reasonable time (approximately 90 days) prior to the expiration.

S. **SMALL BUSINESS SUBCONTRACTING AND EVIDENCE OF COMPLIANCE:**

1. It is the goal of the Commonwealth that 40% of its purchases be made from small businesses. This includes discretionary spending in prime contracts and subcontracts. All potential bidders/offerors are required to submit a Small Business Subcontracting Plan. Unless the bidder/offeror is registered as a DMBE-certified small business and where it is practicable for any portion of the awarded contract to be subcontracted to other suppliers, the contractor is encouraged to offer such subcontracting opportunities to DMBE-certified small businesses. This shall not exclude DMBE-certified women-owned and minority-owned businesses when they have received DMBE small business certification. No bidder/offeror or subcontractor shall be considered a Small Business, a Women-Owned Business or a Minority-Owned Business unless certified as such by the Department of Minority Business Enterprise (DMBE) by the due date for receipt of bids or proposals. If small business subcontractors are used, the prime contractor agrees to report the use of small business subcontractors by providing the purchasing office at a minimum the following information: name of small business with the DMBE certification number, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product/service provided.

2. Each prime contractor who wins an award in which provision of a small business subcontracting plan is a condition of the award, shall deliver to the contracting agency or institution on a quarterly basis, evidence of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the small business subcontracting plan. When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm with the DMBE certification number, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product or service provided. Payment(s) may be withheld until compliance with the plan is received and confirmed by the agency or institution. The agency or institution reserves the right to pursue other appropriate remedies to include, but not be limited to, termination for default.

T. **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.

U. **CONTINUITY OF SERVICES:**

a) The Contractor recognizes that the services under this contract are vital to the Agency and must be continued without interruption and that, upon contract expiration, a successor, either the Agency or another contractor, may continue them. The Contractor agrees:

(i) To exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor;
(ii) To make all Agency owned facilities, equipment, and data available to any successor at an appropriate time prior to the expiration of the contract to facilitate transition to successor; and
(iii) That the Agency Contracting Officer shall have final authority to resolve disputes related to the transition of the contract from the Contractor to its successor.

b) The Contractor shall, upon written notice from the Contract Officer, furnish phase-in/phase-out services for up to ninety (90) days after this contract expires and shall negotiate in good faith a plan with the successor to execute the phase-in/phase-out services. This plan shall be subject to the Contract Officer's approval.

c) The Contractor shall be reimbursed for all reasonable, pre-approved phase-in/phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract. All phase-in/phase-out work fees must be approved by the Contract Officer in writing prior to commencement of said work.

V. **STATE CORPORATION COMMISSION IDENTIFICATION NUMBER:** Pursuant to Code of Virginia, §2.2-4311.2 subsection B, an offeror organized or authorized to transact business in the Commonwealth pursuant to Title 13.1 or Title 50 is required to include in its proposal the identification number issued to it by the State Corporation Commission (SCC). Any offeror that is not required to be authorized to transact business in the Commonwealth as a foreign business entity under Title 13.1 or Title 50 or as otherwise required by law is required to include in its bid a statement describing why the offeror is not required to be so authorized. Indicate the above information on the SCC From provided as Attachment G. Contractor agrees that the process by which compliance with Titles 13.1 and 50 is checked during the solicitation state (including without limitation the SCC Form provided) is streamlined and definitive, and the Commonwealth's use and acceptance of such form, its acceptance of Contractor's statement describing why the offeror was not legally required to be authorized to transact business in the Commonwealth, shall not be conclusive of the issue and shall not be relied upon by the Contractor as demonstrating compliance.

W. **PRISON RAPE ELIMINATION ACT (PREA):** Contractors and Contractors' staff, who are providing services to the Virginia Department of Corrections, who having 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 III

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 Contract Administrator 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 inmates 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 inmate, 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 inmate 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 inmates 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 inmate 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 IV

Operating Procedure

Effective Date July 1, 2010	**Number** 310.2
Amended	**Operating Level** Department
Supersedes Operating Procedure 310.2 (1/1/09)	
Authority COV §53.1-10, §2.2-2010, §2.2-2651, §2.2-2827 BOC None	
Subject **INFORMATION TECHNOLOGY SECURITY**	**ACA Standards** 4-4100, 4-4101, 4-4102; 4-ACRS-7D-05, 4-ACRS-7D-06
Incarcerated Offender Access Yes ☐ No ☒ / **FOIA Exempt** Yes ☐ No ☒ / **Attachments** Yes ☒ #8 No ☐	**Office of Primary Responsibility** 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 SEC501-01. This standard defines the requirements to protect the 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 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 Technology Security group of the Fiscal Administration and Security section of CTSU. 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 Support Associate (**LSA)** - An individual whose primary responsibilities are not related to IT, but provides IT support to others within the same operating unit.

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

Software Applications - Software used by DOC personnel to perform needed job duties (e.g. *VACORIS, CIPPS, 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, CIPPS, 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, CIPPS, etc*.).

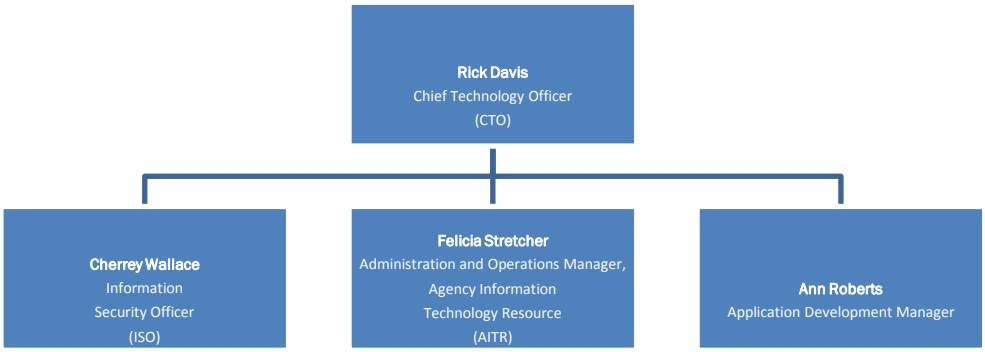
Virus - A program which can replicate itself and infect a computer without the user's knowledge. The difference between a virus and a worm is that a virus requires a host program in order to replicate. A virus can only spread from one computer to another when its host is taken to an uninfected computer 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.

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* (see Attachment 1).

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 VITA/NG through the Virginia Customer Care Center (VCCC).

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* (see Attachment 4) submitted to the VCCC.

b. Each request for a new account must include a *Windows/VMS User Information Security Agreement* (see Attachment 5) 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* (see Attachment 4) submitted to the VCCC.

d. All user re-name account requests must include a *Windows/VMS User Account Request* (see Attachment 4) submitted to the VCCC.

e. All requests for account transfers must be submitted by the receiving location utilizing a *Windows/VMS User Account Request* (see Attachment 4) to the VCCC.

f. All requests for account disables must include a *Windows/VMS User Account Request* (see Attachment 4) submitted to the VCCC.

g. Any user going on a leave of absence expected to last 60 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* (see Attachment 4) submitted to the VCCC by the user's Supervisor.

j. Account deletions should be submitted within 24 hours of an employee or contractor termination.

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* (see Attachment 6) to VCCC. A signed copy of the *Windows/Admin Security Agreement* (Attachment 1) should be sent to CTSU Security.

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.

D. Remote Access (Firepass)

1. 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* (see Attachment 8) sent to CTSU Security.

2. All remote access (Firepass) should use 128 bit or greater encryption.

3. Use of any remote connection to DOC IT Systems constitutes acceptance of and agreement to this 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 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. 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:

   a. The type of access required

   b. Direction of dataflow

   c. Contact information for the organization owning the IT system and/or data, including the System Owner and System Administrator.

   d. 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.

   e. 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 procedure.

4. Non-DOC entities that are granted access are required to sign a *Windows/VMS User Information Security Agreement* (see Attachment 5).

5. Non-DOC entities that are granted Domain Administrator Access must sign the *Windows Admin/System Security Agreement* **(**see Attachment 1**).**

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, CIPPS, FATS, LIDS, CAIS*, etc.) must be sent to and approved by the Software Applications Authorizer listed on the *DOC Applications Access Authorization* (see Attachment 7)**.** (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.

7. ALL software application privileges granted, modified, and/or revoked must be performed by the CTSU Security group or their designee.

8. CTSU Security conducts an annual review of all software applications access approved by Software Applications Authorizers.

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 3) 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 501-01), 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.

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.

   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 Director (e.g. stand alone devices with office automation software or educational devices intended for offender use).*

   The only exception is supervised offenders in the work release program at VCE with explicit approval of the Deputy Director of Administration.

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 procedures. Based on the scope of work to be performed, a background check may be 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.

8. 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. Sending e-mail using another's identity, an assumed name, or anonymously

h. Forwarding of joke e-mail, chain letters, personal photographs, etc.

i. The use of language, words, or pictures that could be considered offensive to others

j. Permitting a non-user to use DOC resources for purposes of communicating the message of some third party individual or organization

k. 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, PDA, etc.) The password should be a pin number with a minimum of 4 digits

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 the VCCC.

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 501-01*.

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) 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 the Inspector General and the Deputy Director for Human Resources.

      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. Deputy Director of Operations, Deputy Director of Administration, Deputy Director of Community Corrections, Deputy Director for Human Resources, Regional Directors, Inspector General, or Communications Manager).

      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. Use of Internet services is a privilege that can be revoked.

   f. 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

   g. 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)

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 the *Employee Standards of Conduct* (see Operating Procedure 135.1).

   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. Allowing access to the Internet, DOC network, LAN, WAN or other network to any person who has not received access approval from the DOC

xii. 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 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.

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.

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 the VCCC to provide assistance in correcting any damage to a desktop personal computer if it becomes infected with a virus.

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. 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* (see Attachment 2. All report information must be e-mailed to the CTSU Security Office (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
   6900 Atmore Drive
   Richmond, Virginia 23225

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 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.

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.

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. The CTO will make appropriate CTSU staff assignments (if needed) within two weeks of receipt of the request. 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. 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.

2. 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) for follow up with the requestor.

3. 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 procedure may be requested through e-mail to the CTSU Fiscal Administration and Security group.

4. Employees and contractors shall NOT allow offenders access (supervised or unsupervised) to software applications that are not stand-alone. Workstations in facilities accessible by offenders must be located in offices or enclosed areas which can be locked and secured. Any exception must be unequivocally approved by the CTO and Deputy Director.

   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 Director (e.g. stand alone devices with CTSU approved office automation software or educational devices intended for offender use).*

   The only exception is supervised offenders in the work release program at VCE with explicit approval from the Deputy Director of Administration.

5. All standalone workstations that have been formerly used by offenders must be reformatted and their operating systems and software reinstalled by contacting the VCCC and opening a ticket prior to attaching the workstation on the DOC network.

6. 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.

7. All files on floppy disks, CD's, 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.

8. Employees and contractors shall NOT allow unauthorized individuals access to DOC

equipment or DOC software applications used for official purposes.

9. 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.

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 procedure. Any IT hardware attached to DOC IT Systems will be subject to this 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 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 the VCCC who will notify CTSU Security staff.

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 connecting to the WLAN must utilize two factor authentication.

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.

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.

E. Security Awareness Training

1. The Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Standard SEC501-01 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, Data Storage Devices, and Media - Prior to its being surplused, 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 SEC501-01, *IT Information Security Standard* (SEC501-01)

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

DHRM Policy #1.75 *Use of Internet and Electronic Communications Systems*

Operating Procedure 135.1, *Employee Standards of Conduct*

IX. REVIEW DATE

The office of primary responsibility shall review this operating procedure annually and re-write it no later than July 1, 2013.

Signature Copy on File

ATTACHMENT V

INMATE BANKING FEES

(Paid by friend or family member transferring funds)

Sending Money With a Credit/Debit Card		
Deposit Amount	**Internet Fee**	**Phone Fee**
$0.01 - $20.00	$2.95	$3.95
$20.01 - $100.00	$5.95	$6.95
$100.01 - $200.00	$7.95	$8.95
$200.01 - $300.00	$9.95	$10.95

Sending Cash at a Walk-In Retail Location	
Deposit Amount	**JPay Fee**
$0.01 - $5,000.00	$4.00 to $7.95*

*Depends on In-Person Location

Sending Money at a Lobby Kiosk		
Deposit Amount	**Cash Fee**	**Credit/Debit Card Fee**
$0.01 - $100.00	$3.00	$5.95

Sending Money Order via Lockbox	
Deposit Amount	**JPay Fee**
$0.01 - $1,000.00	Free