	DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS **POLICY AND PROCEDURE**	**EFFECTIVE DATE:**	August 18, 2023	**Page 1 of 17**
		SUPERSEDES:	2420.4D December 19, 2017	
		OPI:	INFORMATION TECHNOLOGY	
		REVIEW DATE:	August 18, 2024	
		Approving Authority	Thomas Faust Director	
	SUBJECT:	**E-MAIL AND INTERNET USE**		
	NUMBER:	**2420.4E**		
	Attachments:	Attachments A-E		

SUMMARY OF CHANGES:

Section	Change
§4	*The Notice of Non-Discrimination section was revised to reflect new implementations of various D.C. Codes to broaden the protections offered in the Human Rights Act of 1977. These changes aim to strengthen workplace protections, foster diversity, equity and inclusion, and promote fair employment practices.*
	The Office of Government and Public Affairs was revised to the Office of Strategic Communications and Constitute Services (OSC) throughout the policy per the revised DOC Organizational Chart.
§14b.	*Internet Access section was revised to provide detail procedures for access to internet requests.*
§14c.	*Language was added to the Email Use section to provide details on DOC IT process of completing requested email address updates based on name changes.*
§14g	*Entirely new section added to policy detailing DOC IT's procedures for handling Hardware Equipment Requests.*
	New Email and Internet Use Attachments B-E were added to the policy.

APPROVED:

Signature on File

8/18/2023

Thomas Faust, Director ***Date Signed***

1. PURPOSE AND SCOPE. To provide guidelines for acceptable use of the internet and email within the DC Department of Corrections (DOC).

2. POLICY. The DOC provides electronic systems as tools to meet employee's programmatic needs as well as to expedite business communications, reduce paperwork, and automate routine office tasks, thereby increasing productivity and reducing costs.

3. APPLICABILITY

a. This policy applies to all full and part-time employees, contractors, consultants and volunteers who are authorized to use DC Government resources and who have been provided with a user account and authorization to use DC Government Information Technology (IT) resources. Authorized users shall not have any expectation of privacy as to E-mail and Internet use.

b. DOC has software and systems in place that can monitor and record all E-mail and Internet use. DOC security systems are capable of recording (for each and every user) each website visit, chat, newsgroup, E-mail message, and file transfer into and out of its internal network. DOC reserves the right to record and monitor users and usage at any time. DOC OIT monitors access to user's E-mail and Internet activity. DOC managers have access to usage patterns and audit logs via a written request to the (OIT) Manager. Verbal or second party requests will not be honored.

c. All DC government, Office of the Chief Technology Officer (OCTO) and DOC policies relating to intellectual property protection, privacy, misuse of government resources, sexual harassment, data security and confidentiality apply to employee conduct on the internet and when using e-mail.

4. NOTICE OF NON-DISCRIMINATION

a. In accordance with the D.C. Human Rights Act of 1977, as amended, D.C. Official Code § 2-1401.01 et seq., (hereinafter, "the Act") the District of Columbia does not discriminate on the basis of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities,

matriculation, political affiliation, genetic information, disability, source of income, status as a victim of an intrafamily offense, or place of residence or business. Sexual harassment is a form of sexual discrimination that is also prohibited by the Act. In addition, harassment based on any of the above-protected categories is prohibited by the Act. Discrimination in violation of the Act will not be tolerated. Violators will be subject to disciplinary action.

5. PROGRAM OBJECTIVES. The expected results of this program are:

a. Provide instruction and guidance on the proper use and management of e-mail and the internet. The use of e-mail and the internet to conduct official government business should be in a manner that complies with federal and local statutory authorities, DC government policies, and this directive.

b. Provide employees an understanding of the proprietary nature of all information created, sent, or received via DOC's E-mail System.

c. The E-mail and Internet Policy shall be incorporated into employee pre-service training, annual in-service training and the periodic orientation processes.

6. DIRECTIVES AFFECTED

a. **Directives Rescinded**

1) PP 2420.4D E-mail and Internet Use (12/19/17)

b. **Directives Referenced**

1) PP 2420.2 Information Security

7. AUTHORITY

a. DC Law 12-175, Act 12-239
b. DC Code Section § 1-1403
c. DC Code Section § 24-211.02. Powers; promulgation of rules
d. OCTO 0001 Internet Access and Use Policy (12/15/03)
e. OCTO 0002 E-mail Use Policy (10/16/07)
f. District Personnel Manual, Chapter 8, Career Service
g. District Personnel Manual, Chapter 9, Excepted Service
h. District Personnel Manual, Chapter 16, General Discipline and Grievances
i. District Personnel Manual, Chapter 18, Employee Conduct

j. District Personnel Manual, Chapter 38, Management Supervisory Service
k. Collective Bargaining Agreement between the Government of the District of Columbia Department of Corrections and The Fraternal Order of Police Department of Corrections dated September 30, 2005.

8. STANDARDS REFERENCED. None.

9. RESPONSIBILITIES

a. OIT shall ensure agency adherence to DOC E-mail and Internet policy and procedures in conjunction with the OCTO security team.

b. OIT is responsible for the day-to- day control of internet information provided or accessed by DOC employees, and to ensure e-mail services are used for internal and external communication that serves legitimate governmental functions and purposes. OIT shall manage all DOC e-mail accounts.

c. OCTO is responsible for maintenance of the related, resident infrastructure for e-mail and internet access by DOC employees per applicable policies.

d. The Office of Strategic Communications and Constituent Services (OSC), in conjunction with OIT, shall ensure that the information DOC makes available on the internet shall be appropriate for public access and editorially suitable.

e. Employees shall adhere to the provisions of this directive and sign an E-mail and Internet Use Acknowledgement Form (Attachment A) as receipt of its issuance.

10. ALLOWABLE USES OF E-MAIL AND INTERNET

a. Communication and information exchange directly related to the mission, charter, or work tasks of a DC government agency;

b. Research and information exchange in support of standards, analysis, advisory, and professional development activities related to the user's DC government duties;

c. Announcement of DC government laws, procedures, policies, rules, services, programs, information, or activities, subject to the broadcast e-mail requirements described below;

d. Application for, or administration of, contracts or grants for DC government programs or research;

e. Other governmental administrative communications not requiring a high level of security;

f. Interagency and external broadcast correspondence that:

1) Is limited to one hundred (100) recipients or fewer,

2) Is not sent to the group distribution list of any other agency (except for emergency communications), and

3) Does not constitute or contain (as an attachment or otherwise) any inter-agency or external bulletin, newsletter, announcement, promotional material, manual, guide, brochure, or marketing collateral, all of which must be posted on websites and not sent in group emails outside the sender's agency list.

g. Interagency and external broadcast e-mails with distribution greater than one hundred (100) recipients that are authorized in advance by the Director of Communications of the Executive Office of the Mayor (EOM) or the Chief Technology Officer;

h. Mayoral broadcast missives, upon a two (2) hour notice to OCTO or with shorter notice to OCTO, in the discretion of the Director of Communications, EOM;

i. Incidental personal purposes, provided that such use does not:

1) Directly or indirectly interfere with the DC Government operation of computing facilities or electronic mail services,

2) Burden the DC Government with noticeable incremental cost;

3) Interfere with the email user's employment, or other obligations to the DC Government.

11. SPECIFICALLY PROHIBITED USES OF E-MAIL AND INTERNET

a. Any purpose that violates a Federal or DC government law, code, policy, standard or procedure.

b. The advertising or other promotion of any private business enterprise or activity.

c. Transmission or solicitation of information or statements that contain profane language, pander to bigotry, sexism, or other forms of prohibited discrimination, or can in any way be construed as intending to harass or threaten another individual, sexually or otherwise.

d. Any activity with religious or political purposes outside the scope of the user's assigned and authorized governmental duties.

e. Any unauthorized purchase.

f. Sending e-mail under names or addresses other than the employee's own officially designated DC government e-mail address.

g. Adding, removing, or modifying identifying network header information ("spoofing") in an effort to deceive or mislead recipients.

h. Opening any "executable" e-mail attachments (e.g., .exe, .bat, .scr,.vbs) from any source.

i. Sending or forwarding "chain" letters (i.e. requests that ask the receiver to forward the message to multiple recipients).

j. Sending any attachment files larger than 25 megabytes (MB) or as limited by OCTO policies however, staff may send larger files via a One Drive link.

k. Sharing organized District e-mail lists with any person outside the District, except as required by the Freedom of Information Act, subpoena, or other compulsory process.

l. Setting e-mail correspondence to forward automatically to an outside (non-District) address.

m. "Broadcast" e-mails that do not meet the "broadcast" e-mail requirements above.

n. Causing a disruption, obstruction, or burden of network resources.

o. Unauthorized enhancements or add-on software to Outlook (e.g., animations, backgrounds, pictures).

p. Use of non-District e-mail services such as Yahoo or AOL on the District's computer network.

q. Use of non-District file sharing such as (but not limited to) Facebook, Twitter, or other file or picture sharing websites.

r. The intentional or negligent introduction of computer viruses into any DC Government systems; agencies must prevent the introduction of computer viruses into DC government systems and must install District-standard virus-scanning software to check any software downloaded as e-mail attachments.

s. Transmission of sensitive (e.g., confidential) information, unless protected by an approved encryption mode.

t. Conducting government business through private e-mail accounts.

12. SENSITIVE EMAIL TRANSMISSION

a. Sensitive information that is considered privileged under an attorney-client relationship, information subject to the Privacy Act, proprietary information, or other information which must be protected from unauthorized disclosure, shall be protected during transmission as follows:

1) The sender shall be certain that the recipient is properly authorized to receive and view the information.

2) The sender shall clearly identify and mark sensitive (e.g., confidential) messages immediately below the message header (i.e., the Subject, Data, From, and To lines) as:

SENSITIVE/CONFIDENTIAL
INFORMATION
(or)
[ATTORNEY/CLIENT PRIVILEGED
INFORMATION]
Do Not Release to Unauthorized Persons.

13. PROTECTED HEALTH INFORMATION (PHI). PHI must be clearly identified immediately below the message header as Protected Health Information. In addition, the following confidentiality statement shall be incorporated into all e-mail transmissions that contain PHI.

PRIVACY/CONFIDENTIALITY NOTICE (PHI):

The information in this transmission contains protected health information in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This message is intended only for the use of the individual to which it is addressed and contains information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. Violation of Privacy Rules may result in civil and criminal penalties consistent with CFR 164.512(k)(5)(iii). If you are not the intended recipient, please contact the sender by e-mail, fax or phone and destroy all copies of the original message.

14. PROCEDURES

a. General

1) DOC users, including employees and supporting consultants/contractors, shall not engage in any activity or transmit any communication that would reflect unfavorably or be deemed inappropriate by DOC or, conflict with any local laws, regulations, or policies.

2) Use of DOC resources knowingly for illegal activity shall be grounds for immediate termination. DOC shall cooperate with all legitimate law enforcement agencies.

3) In the event that access privileges are misused or abused, supervisors or sponsors of contractors/consultants shall request removal or suspension of access privileges for the individuals involved. Such requests shall be made in writing to OIT.

4) If it is determined that the misuse or abuse constitutes cause for discipline, actions shall be consistent with provisions of the applicable District Personnel Manual (DPM) and the Collective Bargaining Agreement:

   a) Chapter 16 General Discipline and Grievances,
   b) Chapter 8 Career Service,
   c) Chapter 9 Excepted Service Employees,
   d) Chapter 38 Management Supervisory Service, or
   e) Chapter 18, Part I Employee Conduct.

5) E-mail and internet access are for business use; therefore, messages are to be courteous, professional, and business-like. Posting or transmitting material that is obscene, hateful, harmful, malicious, threatening, hostile, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable is prohibited.

6) Monitoring and filtering software shall be installed by OIT, only, to ensure that the desired environment for productive work is provided.

7) Files that are downloaded from the internet or e-mail attachments must be scanned with virus detection software provided by IT before installation and execution. Appropriate precautions shall be taken to detect viruses and to prevent their spread.

8) The truth or accuracy of information on the internet and in e-mail is to be considered suspect, until confirmed by the originator or by a separate reliable source.

9) Solicitation of non-DOC business or any use of the electronic media for personal gain is prohibited.

b. Internet Access

1) Access to the internet requires written approval from the requestor's supervisor and the Administrator (OIT), it is accomplished through LAN workstations, and requires the installation of additional software. Requests, explaining the need for access by specific individuals, are forwarded through supervisory channels to the OIT Chief. Supervisors shall complete the DOC IT Application Access Request Form (Attachment B - sample), sign and email the form to 'DOC.applicationrequest@dc.gov'. VPN access requires completion of the OCTO VPN Access Request form (Attachment C - sample), approval memo from Deputy Director, a completed DOC IT Hardware Request Form (Attachment D - sample) and OIT Chief approval.

2) The request should specifically state the job duties that require access to the application and/or network resource. Completed forms must be signed and submitted by Captains or above (Operations) or Managers (Non-uniformed) via email to: DOC.ApplicationRequest@dc.gov. Please allow up to five (5) business days to process internal application request forms. You will be notified by OIT staff when action has been taken on this request.

3) The internet does not guarantee the privacy or confidentiality of information. Sensitive DOC material may not be transmitted over the

internet, unless it is properly encrypted and pre-approved by senior DOC leadership.

4) DOC provides access to the Internet through the District of Columbia Wide Area Network (DCWAN). Alternate connections to DOC's internal network are not permitted, unless authorized by OIT in advance and in writing.

5) Unless otherwise noted, all software on the internet shall be considered copyrighted. Employees are prohibited from communicating, disseminating, or printing any copyrighted materials in violation of applicable copyright laws. In consideration of DOC's grant of internet access to employees, such employees agree to indemnify and save DOC from any and all claims, demands, liabilities, causes of action, losses, damages and costs (including attorney's fees) arising out of or related to an employee's violation of applicable laws or violation of this policy.

6) All data transmitted becomes the property of DOC. DOC has the right to access, review, copy, and delete any data sent, received, or stored. In addition, DOC reserves the right to disclose this information to any party, whether inside or outside DOC, that DOC deems appropriate, insofar as it is consistent with any applicable local law, HIPPA or any other federal law, regulations, copyrights or licenses, excluding information protected by any privilege.

c. E-mail Use

1) E-mail addresses identify the organization that sent the message; therefore, e-mail is equivalent to letters sent on official letterhead.

2) Users of the DOC E-mail System are expected to follow the same business rules consistent with other written correspondence in terms of addressees, distribution, use of supervisory and administrative chains, and organizational structures.

3) Storage of large numbers of e-mail messages is discouraged, as large numbers of e-mails will negatively impact system performance.

4) DOC's Human Resource will notify IT of an employee's name change and request changes to be made to the employee's(s') email address and other IT records.

5) DOC IT will notify each employee with a pending name change of the new email address, and the effective date and time of change. IT staff shall also provide a list of DOC applications and systems this change will affect. IT staff shall obtain an acknowledgement that the employee is aware of the upcoming change and what system/application/access this change will affect, before making any changes.

d. OIT shall:

1) Serve as DOC liaison with the OCTO.

2) Provide internet access and service for authorized use by DOC employees., Requests made by outside entities, and consultants/contractors shall be granted access to the internet via the DOC network, upon approval by DOC CIO.

3) Provide technical assistance along with managing e-mail accounts of users.

4) Maintain up-to-date master files listing DOC employees, contractors, and consultants who are currently authorized access, maintain historical files of former employees who were previously authorized access, and maintain original signed E-mail and Internet Use Acknowledgement Forms (Attachment A).

5) Ensure that security procedures are current, understood, and that DOC is in compliance with security policy.

6) Install monitoring and filtering software on DOC Networks that is capable of recording (for each and every user) each website visit, each chat room, newsgroup or e-mail message, and each file transfer into and out of DOC's internal networks.

7) Ensure that all information technology and related records are managed in accordance with the Office Accreditation and Compliance (OAC) procedures and Retention and Disposal of Department Records, PS 2000.2. Ensure that no records are destroyed without proper authorization, and that disposition schedules are kept current.

8) Ensure that passwords are changed on a periodic basis, and that the e-mail system reminds authorized e-mail users when it is time change their e-mail password.

9) Monitor e-mail and internet use, and report all suspected violations to the Deputy Director of Administration.

10) Update and maintain DOC's website upon request from other DOC offices.

11) Assist other DOC offices in linking to the DOC website and other internet sites.

e. Warden/Administrators/Office Chiefs shall:

1) Ensure that outside entities, consultants, and contractors supporting them understand, agree, and adhere to the policies related to e-mail and internet use, and submit the original E-mail and Internet Use Acknowledgement Form (Attachment A) to OIT.

2) Report all suspected violations of this policy to OIT.

f. The Office of Strategic Communications, in conjunction with OIT shall:

1) Serve as content manager for the DOC website.

2) Evaluate, approve, and/or disapprove suggested additions and changes related to the DOC website.

3) Ensure that information released to the public represents DC and DOC concerns, and that the information that DOC makes available on the internet is appropriate for public access and editorially suitable. (i.e., appropriate in terms of conformity with Federal, local laws and regulations).

4) Consults with the Office of General Counsel (OGC) when necessary to determine suitability of information for DOC's website.

g. DOC employees and other authorized users shall:

1) Access e-mail messages for the first time in private to protect confidentiality of possibly sensitive information.

2) All e-mail and internet users shall sign the attached statement – Attachment A.

3) Routinely change passwords based on the DC Government/OCTO Web Mail programs or when prompted, and maintain passwords confidentially.

4) Log off and disconnect communication links when workstations are unattended. Failure to logout of internet or e-mail applications shall not relieve an employee of liability for misuse of internet or e-mail resources by someone else.

5) Treat the e-mail and internet systems as if they were a shared file system, with the expectations that messages sent, received, or stored on the servers, or on individual hard drives will be available for review by any authorized representatives of DOC for any purpose.

6) Identify themselves honestly, accurately, and completely when participating in web conferences (such as but not limited to WebEx), or other conference forums or when setting up accounts on outside computer systems.

7) Refrain from chat rooms and other public forums that reveal sensitive information, inmate data, operations procedures, or any other information covered by DOC policies and procedures.

8) Refrain from speaking/writing on behalf of DOC to a newsgroup, the media, to analysts, or to chat rooms in a public gathering or other forums, unless authorized.

9) Follow the guidelines outlined in this directive, and refrain from using the internet to deliberately propagate any virus, worm, Trojan horse, or trap door program code.

10) Report any suspected violations of this directive to their Supervisor.

h. Hardware Equipment Requests:

1) DOC issued hardware equipment requires a written request, and approval from the requestor's supervisor and the Administrator (IT).

2) Requests explaining the need for hardware equipment by specific individuals are forwarded through supervisory channels to the IT Chief. Supervisors shall complete the DOC IT Hardware Request Form – Attachment D, sign and email the form to 'DOC.hardwarerequest@dc.gov', along with all supporting documentation.

a) Supporting Documentation - Printers, scanners Laptop and cellphone – Each request for cellphone, laptop, printer, VPN access and or scanner will require a memo detailing the justification for request and should be submitted for review and approval to the appropriate Deputy Director.

b) Completed forms must be signed and submitted by Captains or above (Operations) or Managers (Non-uniformed) along with the approved memo or email XXXX (if required) via email to: DOC.HardwareRequest@dc.gov.

3) Desktop workstation and other hardware – Requires completion of HW Request Form, and supervisor approval.

i. Equipment Assignment and Return

1) IT staff shall assign equipment available in IT's inventory to the requestor when an approved request is received. When equipment is on back order with suppliers, IT may not have inventory available, and will be able assign one when equipment is received and set-up is complete. IT will notify the requester if the requested equipment is on backorder, and the expected timeframe to complete the request.

2) Cellphones are managed and issued by OCTO and involves processes and timeframes beyond DOC IT control. IT will make a request with OCTO on behalf of the requester and notify the requester when the device is ready and available for issue.

3) IT staff handing off hardware equipment including laptop and cellphone shall obtain a signed receipt of the HW receipt acknowledgement form and provide the requester with a copy.

4) An employee wanting to return equipment for any reason shall return hardware equipment including laptop and cellphone to IT staff at Central Detention Facility (CDF). IT staff receiving the equipment shall inspect the equipment, note any issues or damages, and sign off as having received the returned equipment. A copy of the acknowledgement form shall be provided to the employee returning the equipment. A report (DCDC1) is required for damaged/lost equipment, and employees shall follow the procedures outlined in the Laptop Received/Returned Acknowledgement Form.

5) An employee separating from DOC shall return hardware equipment including laptop and cellphone to IT staff at CDF, HR, or any supervisor within the employee's chain of command. IT staff receiving the equipment shall inspect the equipment, note any issues or damages, and sign off as having received the returned equipment on the Laptop

Received/Returned Acknowledgement Form (Attachment E). A copy of the acknowledgement form shall be provided to the employee returning the equipment. IT staff receiving equipment shall also sign off on the HR Exit form.

Attachments:

Attachment A – Email and Internet Use Acknowledgement Form

Attachment B – DOC IT Application Access Request Form (SAMPLE)

Attachment C – OCTO VPN Access Request Form (SAMPLE)

Attachment D – DOC IT Hardware Equipment Request Form (SAMPLE)

Attachment E – Laptop Received/Returned Acknowledgement Form

DC Department of Corrections

EMAIL AND INTERNET USE ACKNOWLEDGEMENT FORM

I, _____ have received a written copy of the DC Department of Corrections (DOC) Email and Internet Use Policy and Procedure 2420.4. I fully understand the terms of this policy and agree to abide by it.

I realize that the DOC's security software may, for management and security purposes, record the Email and Internet address of each site that I visit and may maintain a record of network activity in which I transmit or receive of any kind of file.

I acknowledge that any message I send or receive will be recorded and stored in an archive file for management's use.

I acknowledge that violation of this policy could result in suspension of my access to the Email and Internet, discipline, employment termination or criminal prosecution.

_____	_____	_____
Name	**Signature**	**Date**
_____	_____	_____
Witness	**Signature**	**Date**

DC DEPARTMENT OF CORRECTIONS
Office of Information Technology
DOC SOFTWARE APPLICATIONS and NETWORK ACCESS REQUEST FORM

PP 2420.2
Attachment B

INSTRUCTIONS AND INFORMATION (PLEASE READ BEFORE COMPLETING THIS FORM)

Use this form to request provisioning or removal of an employee's access rights to DOC network and software applications.

The request should specifically state the job duties that require access to the application and or network resource. Completed forms must be signed and submitted by Captains or above (Operations) or Managers (Non-uniformed) via email to: DOC.ApplicationRequest@dc.gov. Please allow up to 5 business days to process internal application request forms. You will be notified by OIT staff when action has been taken on this request.

External agency application requests (i.e. PRISM, JUSTIS) are dependent upon external agency processes and may take longer. DOC OIT shall make the request on employee's behalf and notify the requestor within 3 business days of receiving a notification from the external agency that the request has been processed. For any queries, please contact the CJCC helpdesk at: Help.Justis@dc.gov.

If you have questions about completing this form, please contact DOC OIT Help Desk: ***202-523-7100****.*

PLEASE DO NOT PRINT THIS FORM. HANDWRITTEN FORMS WILL NOT BE ACCEPTED

Employee Information			
Employee Name:		Title:	
Position:		Location:	
Work Phone:		Work Email:	
Is Employee a Supervisor?:	◯ Yes ◯ No	Post or Office Assigned:	
Employee Status:	◯ New ◯ Reassigned	Previous Post: (if Reassigned)	

SELECT ACCESS REQUESTED FROM BELOW LISTS

1. DOC Applications	List Specific Rights, Profile, Role or Access required
JACCS	
DC Gov Email	
Network (AD)	
Lotus Notes	
Crystal Reports	
NorthPointe	
In-Time	
Other Application:	
Other Application:	

DC DEPARTMENT OF CORRECTIONS
Office of Information Technology
DOC SOFTWARE APPLICATIONS and NETWORK ACCESS REQUEST FORM

2. External Applications (List Specific Rights, Profile, Role or Access required)
☐ JUSTIS/ PRISM (also complete the JUSTIS Application Access Request Form)

PLEASE NOTE: Access to JUSTIS/ PRISM applications are dependent on external agency (CJCC) and processing your application may take longer. Please contact the agency with any questions at: Help.Justis@dc.gov. DOC OIT may not be able to respond to your queries on these applications.

3. Medical and Health Services Administration access only *(All other requests for access require approval of the Deputy Director for Administration)*		
Centricity EMR	Group:	Role:
	Specialty:	Location:

Supervisor Information, Approval and Notes			
Supervisor Name:		Date:	
Comments:		Supervisor Signature:	

Click to email form

*** DOC OIT USE ONLY ***

Request completed by:		**Date Completed:**	
Notes:			

Click to Clear and Reset Form

GOVERNMENT OF THE DISTRICT OF COLUMBIA

OFFICE OF THE CHIEF OF TECHNOLOGY OFICER

CITYWIDE IT SECURITY (CWITS)

ALL REMOTE ACCESS/VPN SERVICE IS RESTRICTED TO DISTRICT GOVERNMENT BUSINESS ONLY. ALL REQUESTS MUST HAVE AGENCY MANAGEMENT APPROVAL PRIOR TO RECEIVING ACCESS AND SUPPORT.

Requestor Instructions: Carefully read the items described on this form and fill in **all** sections. **All sections must be typed, not handwritten, and completed in order to process your request.** Forward the form to your management for signature approval.

Requestor Manager Approver: *This request must be approved and signed by an appropriate CIO or Program Director. This request must be completed in full and submitted for review to CWITS no less than ten (10) business days prior to the access due date*. Send printed completed form with original signature approval to:* **DOC Agency Telecommunications Coordinator (ATC) in the OIT office at the DOC Central Detention Facility, 1901 D Street SE, Washington DC 20003.**
APPROVALS:

Agency Approver Name: Baron Hsu **Approver Title: DOC OIT Manager**
Approver Office Phone #: 202-523-7108 **Action: New VPN access: □ Terminate: □**

Agency Approval Signature: _____Date: _____

Supervisor Signature: _____Date: _____
Supervisor Printed Name: _____

Business Justification for VPN Access:

Last Name:	First Name:	MI:	Last 4 Digits SSN#
Email:		Birth Month:	
Agency: DOC	Agency Group:	Agency POC: Ponti Andrews	Email: DOC_ATC@dc.gov
Home Address:			
City:		State:	Zip:
Office Phone #:		Mobile Phone with SMS (text messaging) #:	

III. USER ACCESS TYPE: (please check one)

Employee □ Contractor □ Temporary □

IV. REMOTE ACCESS USAGE & ACKNOWLEDGEMENT AGREEMENT

By signing, I acknowledge receipt that I have read and understand the District's Remote Access Standards. I understand that I am to use the VPN access assigned specifically to me, solely for the purpose of conducting the official duties of my position. I also understand that I may not attempt to use another's VPN authentication code or device not assigned to me by CWITS. I agree to access only those resources for which I have been authorized and to honor these responsibilities as well as those defined in DC Government's Policies and applicable departmental procedures. I further understand that failure to adhere to such responsibilities may result in access being denied to relevant computer systems and networks. Violators may be subject to penalties, including disciplinary action that includes termination of employment, criminal prosecution and/or other appropriate action.

User Signature: _____ Date: _____
An actual signature is required of the DC Government employee, contractor or other persons receiving a VPN access.

DC DEPARTMENT OF CORRECTIONS
Office of Information Technology
DOC HARDWARE EQUIPMENT REQUEST FORM

PP 2420.4
Attachment D

INSTRUCTIONS AND INFORMATION (PLEASE READ BEFORE COMPLETING THIS FORM)

Use this form to request DOC IT hardware equipment including desktop PCs, laptop, printer, scanner, cellphone and desk phone

Each request for cellphone, laptop, printer, VPN access and or scanner will require a memo detailing the justification for request and should be submitted for review and approval to Deputy Director of Administration.

Completed forms must be signed and submitted by Captains or above (Uniformed) or Managers (Non-uniformed)along with the approved memo (if required) via email to: DOC.HardwareRequest@dc.gov.

Please allow up to 10 business day for processing this request after it is submitted. Cellphones may take longer. Requestor will be notified by OIT staff when action has been taken on this request and OIT shall make the device available for use within 3 business days.

Note: If past 10 days, we may be experiencing delays in receiving hardware shipments from our vendors. DOC OIT shall make the device available to the requestor within 3 business days of receiving shipment.

If you have questions about completing this form, please contact DOC OIT Help Desk: ***202-523-7100.***

PLEASE DO NOT PRINT THIS FORM. HANDWRITTEN FORMS WILL NOT BE ACCEPTED

Employee Information			
Employee Name:		Title:	
Position:		Location:	
Work Phone:		Work Email:	
Is Employee a Supervisor?:	◯ Yes ◯ No	Post or Office Assigned:	
Employee Status:	◯ New ◯ Reassigned	Previous Post: (if Reassigned)	

Hardware Equipment that Requires Approval by a Manager or Captain(or above) (SELECT HARDWARE EQUIPMENT REQUESTED FROM BELOW LIST)	
☐ Desktop PC	☐ Other (specify):
☐ Other (specify):	

Supervisor Information, Approval and Notes			
Supervisor Name:		Date:	
Comments:		Supervisor Signature:	

DC DEPARTMENT OF CORRECTIONS
Office of Information Technology
DOC HARDWARE EQUIPMENT REQUEST FORM

PP 2420.4
Attachment D

Hardware Equipment that Requires Deputy Director Approval (SELECT HARDWARE EQUIPMENT REQUESTED FROM BELOW LIST)			
☐	VPN Access	☐	Laptop
☐	Printer	☐	Mobile/Cellular device (cellphone)
☐	Scanner	☐	Other (specify):

Deputy Director Approvals				
Deputy Director of Administration	◯ Approved ◯ Denied	Signature	Date:	
Deputy Director of Operations	◯ Approved ◯ Denied	Signature	Date:	
Deputy Director of Education,Programs, Case Management, Reentry Services	◯ Approved ◯ Denied	Signature	Date:	

Click to submit form

*** DOC IT USE ONLY ***

Request Completed by:				Date Completed:	
Notes:					
DOC OIT Administrator:	Baron Hsu	◯ Approved ◯ Denied	Signature	Date:	

Issuance of Telecommunication Equipment			
Make Cellular Device Issued:		Model of Cellular Device Issued:	
Cellular Number Issued:		Cellular Device Issued Date:	
Laptop Make Issued:		Laptop Model Issued:	
Date VPN access Issued:		Laptop Issued Date:	

Click to Clear and Reset Form

POLICY AND PROCEDURES FOR LAPTOP USE

1. Users must first complete a request form.

2. To prevent abuse of loaner laptops, a brief training session consisting of the following: 15-minute overview training in the appropriate use of the laptop.

   - Laptop power supply vs. battery use
   - Managing peripheral bay devices such as CD-ROM, USB and battery pack
   - Users will be advised that touching the soft plasma laptop screens with fingers, pens, etc. could cause permanent damage, and therefore they should not touch the delicate screens.
   - Off/On button
   - Volume Control

3. The comprehensive check-in procedure allows easy follow-up with users regarding any mishandling of the returned laptops. Laptops are to be picked and returned on time. If more time is needed the user will need to call to see if an extension can be granted.

4. In case of unsupervised laptops:

   *Under no circumstance should laptops be left in unsupervised area. Please make sure your laptop is secured at all time. Any laptop left in any open area is in danger of being stolen. If **IT** staff finds an **unsupervised** laptop he/she **will confiscate** the laptop and take it to the appropriate office. **Disciplinary** action will be taken*

Violation of the laptop policy, depending on depth and range of the offense, can lead to loss of privileges. Extreme cases will be subject to lost of total privileges using any technical equipment In the case of stolen or lost a report will be given to Internal Affairs the matter will be handled by their investigation.

CARE AND MAINTENANCE

No food or drink is allowed while laptops are in use.

Do not press on the screens or use any cleaning products on the screens. The laptop screens can be damaged if subjected to rough treatment. The screens are particularly sensitive and maybe damaged from excessive pressure on the screen.

Do not lean on the laptop when it is closed. Do not place anything near the laptop that could put pressure on the screen. Do not place anything in the carrying case that will press against the cover. Do not poke the screen. Do not place anything on the keyboard before closing the lid **(pens, pencils, or flashdrives)**.

File sharing programs are not allowed on the laptops. If you are caught with any program like this on your laptop you may loose your loaner privileges. No software is allowed to be installed without authorization from IT.

Virus Protection

The laptops have McAfee Anti-Virus Corporate Edition. This software will scan the hard drive and USB for known viruses on boot up. Each time the user logs onto the laptop.

Claims

A claim for damaged laptops should be reported to the HelpDesk. Each user is responsible for any damage and/or malfunction to laptop. If a laptop becomes lost or stolen a police report needs to be filed. You will then need to send a memorandum to Baron Hsu with the Police Report # and cc: Baron Hsu. Internal Affairs may investigate the matter if DOC policy dictates.

Carrying Laptops

The protective bag will be provided for you to carry the laptop. These bags have sufficient padding to protect the laptop from normal treatment and provide suitable means for carrying the laptop, and paraphineral only. Do not store anything else beside what has accompanied the laptop.

Turn off laptops before placing them in the carrying case.

Laptops are to be picked up from the DOC IT ADP office M-F before 4pm. If you have any questions please do not hesitate to call the DOC HelpDesk at 202.523.7100.

_____ _____
Laptop Received: **Date**

_____ _____
Laptop Returned: **Date**

Signature of IT Technician: _____
Name - J18409
SN#