Idaho Department of Correction	**Standard Operating Procedure** **Division of Management Services** **General Administration**	**Control Number:** 141.03.04.007	**Version:** 1.1	**Page Number:** 1 of 8
				Adopted: 5-12-2010 **Reviewed:** 5-12-2010
		Title: Remote Network Access		

This document was approved by Tony Meatte, chief of the Division of Management Services, on 5/12/10 (signature on file).

BOARD OF CORRECTION IDAPA RULE NUMBER

None

POLICY STATEMENT NUMBER 141

Information Technology Management

POLICY DOCUMENT NUMBER 141

Information Technology Management

DEFINITIONS

Standardized Definitions List

Authentication: The process of proving the identity of a computer or computer user. (E.g., for users it generally involves the use of a user identification [user ID] and password or personal identification number [PIN], and for computers it usually involves the computer passing a code that identifies that it is part of a network.)

Digital Subscriber Line (DSL): Technology that provides a dedicated digital circuit between a residence or business and a telephone company's central office, allowing high-speed data transport over existing twisted copper telephone lines. (E.g., a DSL is widely used to connect to the Internet because of its high speed capability and reasonable cost.)

Integrated Services Digital Network (ISDN): Technology that provides the capability for voice, data, etc. to be converted to a digital signal and transmitted over existing telephone lines. (E.g., An ISDN is an alternative to a digital subscriber line [DSL] but is rarely used for home Internet use because of its expense.)

Internet: An open global network of interconnected commercial, educational, and governmental computer networks that use a common communications protocol such as TCP/IP (transmission control protocol/Internet protocol) to share data.

Manager: An employee appointed to manage, direct, and control a designated work unit. Managers include division chiefs, deputy division chiefs, facility heads, deputy wardens (or second-in-commands), district managers, designated lieutenants, program managers, or any appointed unit manager.

Modem: A device that converts a digital bit stream into an analog signal (and back again) so computers can communicate digitally across analog telephone lines. (Modem is a contraction for MOdulation/DEModulation.)

Pass Phrase: A sequence of words or other text that is (1) used to control access to a computer system, program, or data, and (2) similar to a password in usage but is generally longer for added security.

Personal Identification Number (PIN): A number (usually consisting of four [4] to six [6] digits) that is used in conjunction with user identification (user ID) to complete the login authorization process.

Remote Access: The ability to gain access to a computer or a network from outside a local area or wide area network via the Internet through a desktop, notebook, or handheld computer modem over a regular telephone line or dedicated line such as a digital subscriber line (DSL) or integrated services digital network (ISDN).

Security Token: A small hardware device (sometimes referred to as an authentication token or key fob) that a user carries to authorize access to a computer network through the use of a personal identification number (PIN).

User Identification (User ID): Generally a name, nickname, or alphanumeric value that identifies the user of a computer network and controls the user's access in terms of (1) type (change, read, update or delete), and (2) what data and level of detail can be accessed.

Virtual Private Network (VPN): A private network connection that makes use of the public telecommunications infrastructure, maintaining privacy through the use of tunneling protocol and security procedures.

PURPOSE

The purpose of this standard operating procedure (SOP) is to establish procedures for requesting and responding to Idaho Department of Correction (IDOC) users' requests to obtain, modify, or remove remote access to the IDOC computer network.

SCOPE

This SOP applies to all IDOC employees, contractors, subcontractors, and vendors who need access to **or** use the IDOC computer network from a remote site.

RESPONSIBILITY

Chief of the Division of Management Services

The chief of the Division of Management Services (or designee) is responsible for overseeing and monitoring the provisions provided herein.

Information Technology (IT) Executive Management

IT executive management shall be responsible for implementing this SOP and for ensuring IDOC employees, contractors, subcontractors, and vendors are practicing the guidelines, standards, and procedures provided herein.

Division Deputy Chiefs or Chiefs

Division deputy chiefs **or** chiefs shall be responsible for permitting IDOC employees, contractors, subcontractors, and vendors remote access to the IDOC computer network.

Table of Contents

General Requirements 3

1. Eligibility for Access to the Virtual Private Network (VPN) 3
2. Use of the VPN 3
3. Requesting (i.e., Adding, Modifying, Removing) Remote Access 4
4. Processing Requests for Remote Access or Removal 6

References 8

GENERAL REQUIREMENTS

1. Eligibility for Access to the Virtual Private Network (VPN)

To be approved for access to the IDOC VPN, IDOC employees, contractors, subcontractors, and vendors (hereinafter referred to as ‘remote users’) shall:

- Have an approved background check on file with IDOC Human Resource Services (HRS);
- Read, acknowledge, and abide by IDOC policy 141, *Computer, Electronic Mail, and Internet Use*, with particular regard to the importance of data integrity and confidentiality of IDOC information; and
- Have the applicable division deputy chief **or** chief’s authorization to remote access the VPN.

Note: For the background check, a *Background Investigation Questionnaire* will need to be downloaded from the IDOC’s Website, completed, and submitted to HRS. (The *Relatives and Friends under IDOC Jurisdiction Agreement* that is attached to the questionnaire does not need to be submitted to HRS.)

Note: The remote user’s IDOC manager shall periodically evaluate the remote user’s need to remote access the VPN, and modify or remove access as needed in accordance with section 3.

2. Use of the VPN

To use the IDOC VPN, remote users shall:

- Use a two-factor security token **or** a network user identification (user ID) and pass phrase to gain access to the VPN (as determined by the IT Unit);
- Not record their pass phrase **or** personal identification number (PIN) on the hardware security token (provided a token was issued);
- Not allow unauthorized or unapproved users to access the VPN;
- Re-authenticate and/or disconnect from the network after 30 minutes of inactivity; and
- Notify the IT help desk to address problems encountered with remote access.

3. Requesting (i.e., Adding, Modifying, Removing) Remote Access

To obtain, modify, or remove remote access, the requestor (to include the prospective remote user **or** IDOC manager) shall begin the process by using the following process steps.

Functional Roles and Responsibilities	Step	Tasks
Requestor	1	Download, and save appendix A, *Request for Remote Access or Removal Form*, to your computer. **Note:** The form can be accessed by clicking on the title of the form or by visiting the Electronic Department of Correction (E-Doc). **Note:** If you already have a current form saved on your computer, you may use it. The most current form in use will always be hyperlinked to this SOP or available on E-Doc and can be identified by the date in the footer of the form.
Requestor	2	Ensure that you complete the form fields as described in steps 2A through 2P below and that the information provided is accurate.
Requestor	2A	**'Requested By' field** – Enter the requestor's first and last name.
Requestor	2B	**'Requestor Phone' field** – Enter a phone number that the requestor can be reached on during normal IDOC business hours (i.e., 8:00 am – 5:00 pm mountain time).
Requestor	2C	**'Division/Unit' field** – Enter the IDOC division or unit that the prospective remote user is assigned to **or** will be most associated with.
Requestor	2D	**'Location' field** – Using the drop-down box, select the location that the prospective remote user is assigned to **or** will be most associated with. If the location is not listed in the drop-down box, select the 'other location' box and enter the location.
Requestor	2E	**'Date of Request' field** – Enter the current date in MM/DD/YYYY format.
Requestor	2F	**'Needed By' field** – Enter the date (in MM/DD/YYYY format) that remote access service is needed by, needs to be modified by, or removed by.
Requestor	2G	**'Type of Request' field** – Select the '**new**' box if new services is being requested; select the '**modification**' box if existing service needs to be modified; or select the '**removal**' box if existing services needs to be discontinued.
Requestor	2H	**'Access Same As' field** – If the access you are requesting is identical to another remote user's access, enter that remote user's name **and/or** network user ID.
Requestor	2I	**'Remote User Name' field** – Enter the prospective remote user's first and last name.

Functional Roles and Responsibilities	Step	Tasks
Requestor	2J	**‘Remote User Phone’ field** – Enter a phone number that the prospective remote user can be reached on during normal IDOC business hours (i.e., 8:00 am – 5:00 pm mountain time).
Requestor	2K	**‘Remote User Email’ field** – If the prospective remote user is a vendor, enter the vendor’s company email address. Otherwise, enter the prospective remote user’s IDOC email address.
Requestor	2L	**‘Remote User Address’ field** – Enter the physical address from which the prospective remote user will access the VPN.
Requestor	2M	**‘Need Access to the Following Systems’ field** – Enter any IDOC IT systems that the prospective remote user will require access (e.g., HelpStar, Novell GroupWise, Offender Management-CIS, Offender Management-Reflections, etc.).
		Note: For a complete list of systems, see the appendix attached to SOP 141.03.04.005, *IT Service Desk: Request for Support, Services, and Resolution*.
Requestor	2N	**‘Job Function’ field** – Select the box (employee, contactor/sub, or vendor) that best describes the prospective remote user’s relationship with the IDOC.
Requestor	2O	**‘Computer’ field** – If the prospective remote user is a vendor, select the ‘vendor computer’ box. Otherwise, select the ‘IDOC Computer’ box.
		Note: If the ‘vendor computer’ box is selected, enter the vendor’s company name in the area below the selected box. Also inform the vendor that the computer must be brought into the IT Unit (located at Central Office) to be physically inspected. **Also inform prospective remote users that personal computers will not be used to access the VPN.**
Requestor	2P	**‘Comments’ field** – Enter any additional comments or information that the IT Unit may need to help facilitate your request.
Requestor	3	• Save and print the form; • In the **‘Remote User Signature’ field**, secure the prospective remote user’s signature; and • Forward the hardcopy form to the deputy chief **or** chief of the division indicated in the **‘Division/Unit’ field**.
		Note: Ensure the prospective remote user reads the statement on the form and agrees before he signs the form. **If the prospective remote user does not sign the form, the process ends here until he voluntarily signs.**

Functional Roles and Responsibilities	Step	Tasks
Deputy Chief or Chief	4	• Print first and last name in the **'Authorized Signer Name'** field. • Print title in the **'Authorized Signer Title'** field; • Sign name in the **'Authorized Signature'** field; • Enter IDOC phone number; and • Return the form to the requestor.
		Note: If not approving the request, contact the requestor and inform him of the reason(s). **The process will then end here.**
Requestor	5	If the form is returned with the deputy chief or chief's signature approval, fax **or** hand-deliver the signed form to the IT help desk for processing in accordance with section 4 of this SOP.
		Note: The fax number is located at the top of the form. If faxed, you may want to follow up with a phone call **or** email to the helpdesk to confirm receipt.

4. Processing Requests for Remote Access or Removal

After the IT helpdesk receives a division deputy chief **or** chief signed *Request for Remote Access or Removal Form,* the following process steps shall be used.

Functional Roles and Responsibilities	Step	Tasks
IT Help Desk Staff	1	Review the received *Request for Remote Access or Removal Form* to determine whether or not the request is complete **and** the proper signature approval was obtained.
		Note: If the form is incomplete **or** the proper signature approval was not obtained, return the form to the requestor to correct. **The process ends here until the form is complete and has the proper signature approval.**
IT Help Desk Staff	2	**Note:** In accordance with SOP 141.03.04.005, *IT Helpdesk Request for Support, Services, and Resolution,* the urgency (priority level) for this type request shall be 'low priority' and an 'initial response' provided within 48 hours of receipt.
		Log into the HelpStar system and enter a new work order. Ensure the 'type of request' (new, modification, or removal), as provided on the form, is also provided on the work order.
		Note: If needed, SOP 141.03.04.005 is a good resource to use for information on how to enter the new work order.
IT Help Desk Staff	3	• Record the work order number on the received *Request for Remote Access or Removal Form* (complete the '**HelpStar WO No.**' field as provided in the 'Information Technology Use Only' section of the form); • Dispatch the IT support resource.

Functional Roles and Responsibilities	**Step**	**Tasks**
IT Support Resource	4	• Monitor the HelpStar system dispatch queue for assigned requests; • Obtain the received *Request for Remote Access or Removal Form* from the IT helpdesk staff; and • In accordance with SOP 141.03.04.005, *IT Helpdesk Request for Support, Services, and Resolution,* process the work order within the 120 'resolution/escalation hours'. ♦ If the type of request is '**new**', proceed to step 5. ♦ If the type of request is '**modification**' skip to step 6. ♦ If the type of request is '**removal**' skip to step 7.
IT Support Resource	5	• To add a **[new]** remote access, determine the appropriate 'access type' (security token, virtual private network, sporlash [a type of encryption], etc.); ♦ **Security token needed** – assign a token and PIN, and update the inventory list. ♦ **VPN or other needed** – assign a user ID and pass phrase. • If the prospective remote user is a vendor, arrange for the user to bring his computer into the IT Unit to be physically inspected; and • Skip to step 8.
IT Support Resource	6	• To change (**modify**) remote access, modify the remote user's VPN account in accordance with the form; and • Skip to step 9.
IT Support Resource	7	• To **remove** remote access, determine what type of access was provided (e.g., security token, virtual private network, sporlash, etc.); ♦ **Security token provided** – remove security token assignment, return token to the inventory, and update the inventory list. ♦ **VPN or other provided** – Delete the account. • Skip to step 9.
IT Support Resource	8	Train the prospective remote user on: • The login process; • Use of the VPN (see section 2 of this SOP);.and • Risks and responsibilities associated with accessing the VPN. **Note:** If the user is a vendor, ensure that the vendor brought his computer into the IT Unit to be physically inspected. Do not proceed to step 9 until the computer is inspected.

Functional Roles and Responsibilities	Step	Tasks
IT Support Resource	9	As applicable, when access has been granted **and** the prospective remote user has received training (if they had not previously been trained): • Answer question #1, located in the ‘Information Technology Use Only’ section of the received *Request for Remote Access or Removal Form.* **(Not required for a removal of remote access)**; • Sign the form and forward to the IT operations manager; and • Update the HelpStar system with resolution information.
IT Operations Management	10	• Answer questions #2 thru 4, located in the ‘Information Technology Use Only’ section of the received *Request for Remote Access or Removal Form.* **(Not required for a modification or removal of remote access)**; • If all approval requirements **have not** been met – ensure the missing approval(s) is/are obtained before proceeding with the next task; or • If all approval requirements **have** been met – sign the form and file; and • Confirm approval and access with the remote user.
		Note: The completed and approved form must be scanned and filed in a network drive location designated by IT operations management, and the original must be maintained in a designated network analyst’s files. One (1) year after access is removed, all request and removal forms pertaining to the remote user and his initial request may be deleted and shredded.

REFERENCES

Appendix A, *Request for Remote Access or Removal Form*

– End of Document –