

**Remote Access Procedures
(VPN, Dial-In, and SecurID)
DIT-TS-310-002**

**Remote Access Procedures
(VPN and Dial-in)**

Date: **February 8, 2005**

To: Telecommunication Services

Priority: 1

Effective Date: April 2005

Training Time: N/A

Related Documents: Local Government Extranet (LGNET)
Operations Guidelines
Procedure 1410.20 – Client Firewall
Procedure 1410.21 – Client VPN
Procedure 1410.22 – External Gateway VPN
Procedure 1410.24 – Internal Gateway VPN

Issuing Department: Telecommunication Services

Author: Christopher Fellows
NOC Remote Access Analyst – (517) 241-1786

Document Owner: Dave Al-Ashari – (517) 241-7382

Revision Number: 3

Table Of Contents

1.0 Overview 5

2.0 Service Offerings..... 5

 2.1 Dial-In..... 5

 2.2 Client VPN..... 6

 2.3 SecurID 7

 2.4 Understanding Costs 7

3.0 Requesting/Changing/Canceling Service..... 7

 3.1 DIT - 0051 areas of responsibility 8

 3.2 Documentation Flow example 8

 3.3 DIT-0051 examples 8

 3.3.1 Requesting new service..... 9

 3.3.1a Explanation of form information 10

 3.3.2 Canceling existing service 11

 3.3.2a Explanation of form information 12

 3.3.3 Changing existing service 13

 3.3.3a Explanation of form information 14

 3.3.4 Reissue (replacement) of defective token 15

 3.3.4a Explanation of form information 16

 3.3.5 Billing changes only requests 17

 3.3.5a Explanation of form information 18

 3.3.6 Reissue (replacement) of lost or expired token..... 19

 3.3.6a Explanation of form information 20

 3.4 DIT-0051 Answers to Frequently Asked Questions (FAQ) 21

 3.4.1 General..... 21

 3.4.2 Vendor specific 21

 3.5 Picking up or dropping off SecurID tokens 21

 3.5.1 Security check at pickup 22

4.0 Remote access configurations (step by step) 22

 4.1 SecurID (setting the PIN)..... 22

 4.1.1 Dialing in via a modem..... 22

 4.1.2 Via the Internet 24

 4.2 Setting up Dial-In (Dialup networking)..... 24

 4.2.1 On Windows XP 24

 4.2.2 On Windows 2000 25

 4.2.3 On Windows NT 25

 4.3 Setting up the VPN client 26

 4.3.1 Installing the VPN client on Windows XP/2000/NT..... 27

 4.3.2 Logging in to the VPN..... 27

 4.3.3 VPN Notes 28

5.0 Troubleshooting 28

 5.1 SecurID 28

 5.2 Dial-In..... 30

 5.3 VPN..... 31

6.0 CSC(Client Service Center) Procedures..... 32

- 6.1 Processing Requests..... 32
 - 6.1.1 New/Change/Cancel 32
 - 6.1.2 Transfer 32
- 6.2 Working Problems 32
 - 6.2.1 Re-synchronization 32
 - 6.2.2 PIN Resets..... 33
 - 6.2.3 When that doesn't work 33

Appendix I 34

- Billing code requirements for DIT-0051 by agency 34

Appendix II..... 35

- Remote Access Request Form DIT-0051 35

Appendix III 36

- Dial Up Connection with VPN 36
- Single User Broadband Connection..... 37
- Multiple User Broadband Connection 38

1.0 Overview

The State of Michigan remote access service is intended for use by state employees and approved vendors to gain access to State of Michigan information technology assets from remote locations to perform State of Michigan business. This access comes in two forms, Dial-in (sometimes referred to as ROAM) and Client Virtual Private Network or Client VPN. Acquiring these services requires following a somewhat convoluted process that can be confusing and time consuming. It involves several individuals to perform various tasks that insure the security, availability, and financial accuracy of state assets. This document is intended for both the end users and the administrators of these programs/services and will attempt to clarify all the procedures required to request, install, and troubleshoot each of the services.

2.0 Service Offerings

There seems to be a fair amount of confusion on what is required to gain access and what you get when you have access over each of these services. With that in mind our first task is to compare and contrast the two services offered by the Department of Information Technology.

2.1 Dial-In

Definition:

Asynchronous data connection over Public Switched Telephone Network (PSTN) and utilizing Point-to-Point Protocol (PPP) to state owned Point of Presence (PoP) locations around the state. Client configuration is accomplished via Dynamic Host Configuration Protocol (DHCP).

In English:

This service is available to users who wish to connect to the state directly. It is basically the same type of service offered by Internet Service Providers (ISP) the world over. A user (client) connects to the state networks via a modem to a bank of modems owned by the state. The client computer is given an Internet Protocol (IP) address and other configuration information as he/she logs in.

Cost:

This service is currently \$15.00 per month per user plus the cost of a SecurID token (\$6.00)

Requirements:

- A computer running a modern operating system (OS) (Windows 2000/XP are supported by DIT) with a modem installed and configured
- A telephone line and connection cables
- A SecurID token card for authentication
- A signed acceptable use policy letter

Features:

- Low speed (56Kb max) point-to-point (non-shared) connection
- No special client side software required
- Lower cost (currently \$21.00 per month per user. \$15.00 for Dial-in and \$6.00 for SecurID token)
- Some applications may not function as expected due to speed constraints of telephone lines

2.2 Client VPN

Definition:

Encrypted data connection over the public Internet utilizing Internet Protocol Security (IPSEC) and terminating on the State of Michigan (SoM) Demilitarized Zone (DMZ). Client configuration is accomplished via Dynamic Host Configuration Protocol (DHCP).

In English:

This connection uses the Internet as its network cable. Information sent over a connected VPN is scrambled so that no one on the public Internet can read your messages as they go back and forth. The client computer is given an Internet Protocol (IP) address and other configuration information as he/she logs in.

Cost: This service is currently \$15.00 per month per user plus the cost of a SecurID token (\$6.00)

Requirements:

- A computer running a modern operating system (OS) (Windows 2000/XP are supported) with a Network Interface Card (NIC) installed and configured
- An Internet Service Provider (ISP)
- A SecurID token card for authentication
- A VPN Client Dialer application (Cisco VPN client) installed and configured
- A signed acceptable use policy letter

Features:

- High speed. Only limited by the connection speed to the Internet
- High encryption/security. Information is sent and received by the highest available encryption method (3DES)
- Portable. Can connect from anywhere in the world that you can connect to the Internet.
- Higher cost. (Currently \$21.00 per month per user plus X dollars per month for Internet access)

2.3 SecurID

A SecurID token card is required for all remote access services. It is important to note that a SecurID token provides authentication only and not access. It is also important to note that there is a separate charge of \$6.00 per month for SecurID.

2.4 Understanding Costs

Confusion is rampant on this subject. Here is the break down. All prices are per month per user.

SecurID Token = \$6.00

Dial-In service = \$15.00

VPN service = \$15.00

Lost Token = \$70.00

So, if you order service for Jane Doe and request Dial-in and VPN access your total bill would be \$36.00 per month for Jane. If later Jane decided that she didn't need Dial-In then the cost would drop to \$21.00 per month. This only takes into consideration the costs charged by DIT. Jane's Internet Service Provider (ISP) charges will be above and beyond the DIT charges. Note: These are subject to change and are accurate as of the date of this publication.

3.0 Requesting/Changing/Canceling Service

All service requests start with a DIT form 0051. This form is available via the web at <http://www.michigan.gov/ditservice> (Follow the quick link to Remote access process) and can be filled out electronically or printed and completed manually. Use this form to accomplish any SecurID task, including:

- Ordering new service
- Canceling existing service
- Changing existing service
- Transferring SecurID tokens between users
- Replacing a defective token

A DIT-0051 is required for every SecurID transaction. What this means is that if you want to transfer a token from one user to another it would require two forms, one to cancel users "A" service and one to request service for user "B". This may seem like double documentation but it is the only way to insure that you don't get double billed. There may be other transactions that seem like they wouldn't require a form, such as a user name change. The problem here is that a Remedy ticket would not be opened and we would not be able to schedule the work. So, the rule of thumb is, if it has to do with a SecurID then break out the forms and fire up the fax machine.

3.1 DIT - 0051 areas of responsibility

The following table breaks down the DIT-0051 into area of responsibility. Again, this is only a guideline and agencies can vary this information to suit individual requirements.

Section(s)	Person/Office of Responsibility
I and II	End User or designated authority
III and V	Person/Office with authority to authorize expenditure of funds
IV	Department Security administrator or authorized requestor
Helpdesk use only	CSC(Client Service Center) personnel
NOC Security use only	DIT Security personnel

3.2 Documentation Flow example

The routing of the DIT form 0051 may vary wildly from agency to agency depending on agency requirements the following example is only a guideline and can be modified to suit individual agency needs. The bottom line of this example is that the CSC requires a completed DIT-0051.

The user initiates the process by identifying his/her requirements in sections I and II. He then forwards the form to the Division Director or whomever is designated the authority to pay for the service. That individual completes his/her sections, signs the form and forwards it to the security administrator. The Security administrator verifies that a signed acceptable use policy letter is on file, checks that the access requested is proper and required, signs and Faxes the completed form to the CSC(Client Service Center) at 517-241-8016. The CSC receives and verifies that the required fields are complete on the form and opens a Remedy case and assigns it to the DIT SC Service. They also enter the Remedy case number on the form. The CSC processes the request from Remedy and closes the case. They also enter the required information on the DIT-0051 and forward the complete form to the NOC Financial team for billing changes.

3.3 DIT-0051 examples

The following section provides examples of which fields need to be filled out on the DIT-0051 to accomplish various SecurID tasks. The CSC (Client Service Center) should also use these examples for Remedy ticket entries. The darkened fields are required for the transaction listed.

3.3.1 Requesting new service

REMOTE ACCESS SERVICE REQUEST
Michigan Department of Information Technology

SECTION I – EMPLOYEE INFORMATION (CARD HOLDER)												
1. Last Name Doe			First Name John			Init 0	2. Email Address doe@michigan.gov					
3. Agency / Office / Division / Section / Unit DIT/Telecommunications/Network Operations/Security												
4. Business Street Address 608 W Allegan Street					5. Business City Lansing			State MI		Zip 48913		
6. Business Phone No. (517) 555-1212			Extension 1234		7. Last 4 digits SS# 9876			8. Birth Date (month & day only-mmdd) 01/01				
9. State User Access <input checked="" type="checkbox"/> State Employee <input type="checkbox"/> Contractor / Company Name							10. Vendor Access Vendor Company Name					
SECTION II – SERVICE REQUESTED												
1. Access Requested <input type="checkbox"/> SecurID Only <input checked="" type="checkbox"/> Dial-in <input checked="" type="checkbox"/> VPN If checked, VPN Group VPN Name if known <input type="checkbox"/> Both <input type="checkbox"/> User GW-toGW - RGWSUVPN <input type="checkbox"/> Vendor GW-to-GW - RGWVVPN Labor Units _____ Code <u>NLROAM</u>												
2. Firewall Access requested: Destination, TCP/IP Port Source = (will be assigned by NOC) Destination = IP Address(es) of systems that need to be reached with this connection. I.e. 10.1.1.1 and 192.168.1.1 Port(s) = Comm ports used in this connection i.e. FTP, HTTP, SQL, etc.												
3. Change Access Type – Existing assigned token only Add: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN Remove: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN												
4. Reissue – No Division Approval required for reissue <input type="checkbox"/> Reissue												
5. Cancel Token (Check appropriate reason) <input type="checkbox"/> Lost <input type="checkbox"/> No longer needed						6. Token Serial # / Tunnel Name			<input type="checkbox"/> Expired <input type="checkbox"/> Defective / Damaged			
SECTION III – DIVISION APPROVAL												
1. Division Approver Name Lotsa Cash						2. Telephone Number (517) 555-5555						
3. Division Approver Signature MUST BE SIGNED						Date 01/01/05						
SECTION IV – DEPARTMENT SECURITY ADMINISTRATOR APPROVAL												
1. Security Administrator Name Iam D'Man						2. Telephone Number (517) 555-9876						
3. Security Administrator Approval Signature MUST BE SIGNED						Date 01/01/05						
SECTION V – BILLING INFORMATION												
1a. Ag Code XXX	1b. Index XXXX	1c. PCA XXXXXX	1d. COBJ XXXX	1e. AOBJ XXXX	1f. Project # XXXX	1g. Prj Ph XXXX	1h. Grant # XXXX	1i. Grt Ph XXXX	1j. Ag 1 XXXX	1k. Ag 2 XXXX	1l. Ag 3 XXXX	
When the above information has been completed, fax this form to (517) 241-8016.												
HELP DESK USE ONLY												
1. Ticket Number			2. Assigned by:						3. Date			
NOC SECURITY USE ONLY – NEW CARD												
4. Token Serial #			5. SecurID Administrator Signature (Required)						6. Start Date			
NOC SECURITY USE ONLY – CANCEL CARD Note: DIT will continue to charge Agency until card is returned or reported lost												
7. Token Received by Signature						8. End Date						

3.3.1a Explanation of form information

Purpose: The proceeding form is used to request new service. Dial-In, VPN, or Both can be requested in this manner.

Specific field information:

SECTION I

Block(s) 1-10 = General user data. All fields must be complete

SECTION II

Block(s) 1 = This is the area where you tell us what type of access you are requesting. Check any boxes that apply, in other words, if you are requesting Dial-In , VPN or Both you would check only the boxes that apply. If the VPN group is known fill in the VPN group name block. (SoMGUVPN, IBMVENDOR, etc.)

Block(s) 2 = This is primarily for Vendor VPNs but may also be used for user connections if destination rules need to be added. This area holds the IP addresses and port numbers (FTP, Telnet, SQL) for the State of Michigan resources that the end user will need to reach via the connection. (GroupWise servers, file servers, print server etc.)

SECTION III

Block(s) All = This area must be completed by the individual or group in your agency that has been granted authority to expend the financial resources required to pay for the service. A signature is required or the form will be rejected by CSC.

SECTION IV

Block(s) All = This area must be completed by the individual or group in your agency that has been identified as the security authority for your agency by the enterprise security office. This person is often referred to as the *Authorized Requestor* and the list, maintained by OES, called *Authorized Requestor List by Agency and Category* may be obtained from that office. A signature is required or the form will be rejected by CSC.

SECTION V

Block(s) 1a – 1l = The billing codes to be used to pay for the service. The minimum blocks are 1a through 1c but some agencies require additional blocks be completed. Please refer to Appendix I for specific agency requirements

The remainder of the form is used exclusively by DIT and need not be completed by agency personnel.

3.3.2 Canceling existing service

REMOTE ACCESS SERVICE REQUEST
Michigan Department of Information Technology

SECTION I – EMPLOYEE INFORMATION (CARD HOLDER)														
1. Last Name Doe			First Name John				Init Q	2. Email Address [REDACTED]						
3. Agency / Office / Division / Section / Unit														
4. Business Street Address						5. Business City			State		Zip			
6. Business Phone No. ()				Extension		7. Last 4 digits SS#			8. Birth Date (month & day only-mmdd)					
9. State User Access <input type="checkbox"/> State Employee <input type="checkbox"/> Contractor / Company Name								10. Vendor Access Vendor Company Name						
SECTION II – SERVICE REQUESTED														
1. Access Requested <input type="checkbox"/> SecurID Only <input type="checkbox"/> Dial-in <input type="checkbox"/> VPN If checked, VPN Group <input type="checkbox"/> Both <input type="checkbox"/> User GW-toGW - RGWSUVPN <input type="checkbox"/> Vendor GW-to-GW - RGWVVPN Labor Units _____ Code <u>NLROAM</u>														
2. Firewall Access requested: Destination, TCP/IP Port														
3. Change Access Type – Existing assigned token only Add: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN Remove: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN														
4. Reissue – No Division Approval required for reissue <input type="checkbox"/> Reissue														
5. Cancel Token (Check appropriate reason)						<input checked="" type="checkbox"/> Lost			<input checked="" type="checkbox"/> Expired			6. Token Serial # / Tunnel Name [REDACTED]		
						<input checked="" type="checkbox"/> No longer needed			<input checked="" type="checkbox"/> Defective / Damaged					
SECTION III – DIVISION APPROVAL														
1. Division Approver Name							2. Telephone Number ()							
3. Division Approver Signature							Date							
SECTION IV – DEPARTMENT SECURITY ADMINISTRATOR APPROVAL														
1. Security Administrator Name							2. Telephone Number ()							
3. Security Administrator Approval Signature							Date							
SECTION V – BILLING INFORMATION														
1a. Ag Code	1b. Index	1c. PCA	1d. COBJ	1e. AOBJ	1f. Project #	1g. Prj Ph	1h. Grant #	1i. Grt Ph	1j. Ag 1	1k. Ag 2	1l. Ag 3			
When the above information has been completed, fax this form to (517) 241-8016.														
HELP DESK USE ONLY														
1. Ticket Number			2. Assigned by:						3. Date					
NOC SECURITY USE ONLY – NEW CARD														
4. Token Serial #			5. SecurID Administrator Signature (Required)						6. Start Date					
NOC SECURITY USE ONLY – CANCEL CARD Note: DIT will continue to charge Agency until card is returned or reported lost														
7. Token Received by Signature							8. End Date							

3.3.2a Explanation of form information

Purpose: The proceeding form is used to cancel remote access service. Dial-In, VPN, Both, or SecurID tokens can be cancelled in this manner. Note: Cancelled token request will not be processed by DIT/CSC until the token card has been returned to CSC.

Specific field information:

SECTION I

Block(s) 1-10 = General user data. Only the users name is required

SECTION II

Block(s) 5 and 6 = Check the reason for the cancellation and enter the token serial number

SECTION III

Block(s) All = Not required

SECTION IV

Block(s) All = Not required

SECTION V

Block(s) All = Not required

The remainder of the form is used exclusively by DIT and need not be completed by agency personnel.

3.3.3 Changing existing service

REMOTE ACCESS SERVICE REQUEST
Michigan Department of Information Technology

SECTION I – EMPLOYEE INFORMATION (CARD HOLDER)												
1. Last Name Doe			First Name John			Init Q	2. Email Address					
3. Agency / Office / Division / Section / Unit												
4. Business Street Address						5. Business City			State		Zip	
6. Business Phone No.				Extension		7. Last 4 digits SS#			8. Birth Date (month & day only-mmdd)			
9. State User Access State Employee <input type="checkbox"/> Contractor / Company Name							10. Vendor Access Vendor Company Name					
SECTION II – SERVICE REQUESTED												
1. Access Requested <input type="checkbox"/> SecurID Only <input type="checkbox"/> Dial-in <input type="checkbox"/> VPN If checked, VPN Group <u>VPN Name if known</u> <input type="checkbox"/> Both <input type="checkbox"/> User GW-toGW - RGWSUVPN <input type="checkbox"/> Vendor GW-to-GW - RGWVVPN Labor Units _____ Code <u> </u> NLROAM _____												
2. Firewall Access requested: Destination, TCP/IP Port Source = (will be assigned by NOC) Destination = IP Address(es) of systems that need to be reached with this connection. I.e. 10.1.1.1 and 192.168.1.1 Port(s) = Comm ports used in this connection i.e. FTP, HTTP, SQL, etc.												
3. Change Access Type – Existing assigned token only Add: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN Remove: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN												
4. Reissue – No Division Approval required for reissue <input type="checkbox"/> Reissue												
5. Cancel Token (Check appropriate reason) <input type="checkbox"/> Lost <input type="checkbox"/> Expired <input type="checkbox"/> No longer needed <input type="checkbox"/> Defective / Damaged						6. Token Serial # / Tunnel Name						
SECTION III – DIVISION APPROVAL												
1. Division Approver Name Lotsa Cash						2. Telephone Number (517) 555-5555						
3. Division Approver Signature MUST BE SIGNED						Date 01/01/05						
SECTION IV – DEPARTMENT SECURITY ADMINISTRATOR APPROVAL												
1. Security Administrator Name Iam D'Man						2. Telephone Number (517) 555-9876						
3. Security Administrator Approval Signature MUST BE SIGNED						Date 01/01/05						
SECTION V – BILLING INFORMATION												
1a. Ag Code XXX	1b. Index XXXX	1c. PCA XXXXXX	1d. COBJ 	1e. AOBJ 	1f. Project # 	1g. Prj Ph 	1h. Grant # 	1i. Grt Ph 	1j. Ag 1 	1k. Ag 2 	1l. Ag 3 	
When the above information has been completed, fax this form to (517) 241-8016.												
HELP DESK USE ONLY												
1. Ticket Number			2. Assigned by:						3. Date			
NOC SECURITY USE ONLY – NEW CARD												
4. Token Serial #			5. SecurID Administrator Signature (Required)						6. Start Date			
NOC SECURITY USE ONLY – CANCEL CARD Note: DIT will continue to charge Agency until card is returned or reported lost												
7. Token Received by Signature						8. End Date						

3.3.3a Explanation of form information

Purpose: The proceeding form is used to change existing service. Dial-In, VPN, or Both can be changed in this manner.

Specific field information:

SECTION I

Block(s) 1-10 = General user data. Only user name is required

SECTION II

Block(s) 1 = Only used if you are moving a user from one VPN group to another

Block(s) 2 = Only used if you need to add or removed destinations to an existing VPN group

Block(s) 3 = Check the boxes that apply to the action you are trying to accomplish. Check all boxes that apply. For example if you wanted to add VPN and remove Dial-In from a user you would check Remove Dial-In/ROAM and check Add VPN.

SECTION III

Block(s) All = This area must be completed by the individual or group in your agency that has been granted authority to expend the financial resources required to pay for the service. A signature is required or the form will be rejected by CSC.

SECTION IV

Block(s) All = This area must be completed by the individual or group in your agency that has been identified as the security authority for your agency by the enterprise security office. This person is often referred to as the *Authorized Requestor* and the list, maintained by OES, called *Authorized Requestor List by Agency and Category* may be obtained from that office. A signature is required or the form will be rejected by CSC.

SECTION V

Block(s) 1a – 1l = The billing codes to be used to pay for the service. The minimum blocks are 1a through 1c but some agencies require additional blocks be completed. Please refer to Appendix I for specific agency requirements

The remainder of the form is used exclusively by DIT and need not be completed by agency personnel.

3.3.4 Reissue (replacement) of defective token

REMOTE ACCESS SERVICE REQUEST
Michigan Department of Information Technology

SECTION I – EMPLOYEE INFORMATION (CARD HOLDER)												
1. Last Name Doe			First Name John			Init 0	2. Email Address					
3. Agency / Office / Division / Section / Unit												
4. Business Street Address						5. Business City			State		Zip	
6. Business Phone No.				Extension		7. Last 4 digits SS#			8. Birth Date (month & day only-mmdd)			
9. State User Access State Employee <input type="checkbox"/> Contractor / Company Name							10. Vendor Access Vendor Company Name					
SECTION II – SERVICE REQUESTED												
1. Access Requested <input type="checkbox"/> SecurID Only <input type="checkbox"/> Dial-in <input type="checkbox"/> VPN If checked, VPN Group _____ <input type="checkbox"/> Both <input type="checkbox"/> User GW-toGW - RGWSUVPN <input type="checkbox"/> Vendor GW-to-GW - RGWVVPN Labor Units _____ Code <u>NLROAM</u>												
2. Firewall Access requested: Destination, TCP/IP Port												
3. Change Access Type – Existing assigned token only Add: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN Remove: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN												
4. Reissue – No Division Approval required for reissue <input checked="" type="checkbox"/> Reissue												
5. Cancel Token (Check appropriate reason) <input type="checkbox"/> Lost <input type="checkbox"/> Expired <input type="checkbox"/> No longer needed <input type="checkbox"/> Defective / Damaged						6. Token Serial # / Tunnel Name						
SECTION III – DIVISION APPROVAL												
1. Division Approver Name Lotsa Cash						2. Telephone Number (517) 555-5555						
3. Division Approver Signature MUST BE SIGNED						Date 01/01/05						
SECTION IV – DEPARTMENT SECURITY ADMINISTRATOR APPROVAL												
1. Security Administrator Name Iam D'Man						2. Telephone Number (517) 555-9876						
3. Security Administrator Approval Signature MUST BE SIGNED						Date 01/01/05						
SECTION V – BILLING INFORMATION												
1a. Ag Code	1b. Index	1c. PCA	1d. COBJ	1e. AOBJ	1f. Project #	1g. Prij Ph	1h. Grant #	1i. Grt Ph	1j. Ag 1	1k. Ag 2	1l. Ag 3	
XXX	XXXX	XXXXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	
When the above information has been completed, fax this form to (517) 241-8016.												
HELP DESK USE ONLY												
1. Ticket Number				2. Assigned by:				3. Date				
NOC SECURITY USE ONLY – NEW CARD												
4. Token Serial #				5. SecurID Administrator Signature (Required)				6. Start Date				
NOC SECURITY USE ONLY – CANCEL CARD Note: DIT will continue to charge Agency until card is returned or reported lost												
7. Token Received by Signature							8. End Date					

3.3.4a Explanation of form information

Purpose: The proceeding form is used to replace a defective SecurID token.

Specific field information:

SECTION I

Block(s) 1-10 = General user data. All fields must be complete.

SECTION II

Block(s) 1-3 = Not required

Block(s) 4 = Check the reissue box

SECTION III

Block(s) All = Not required.

SECTION IV

Block(s) All = This area must be completed by the individual or group in your agency that has been identified as the security authority for your agency by the enterprise security office. This person is often referred to as the *Authorized Requestor* and the list, maintained by OSD, called *Authorized Requestor List by Agency and Category* may be obtained from that office. A signature is required or the form will be rejected by CSC.

SECTION V

Block(s) 1a – 1l = The billing codes to be used to pay for the service. The minimum blocks are 1a through 1c but some agencies require additional blocks be completed. Please refer to Appendix I for specific agency requirements

The remainder of the form is used exclusively by DIT and need not be completed by agency personnel.

3.3.5 Billing changes only requests

REMOTE ACCESS SERVICE REQUEST
Michigan Department of Information Technology

SECTION I – EMPLOYEE INFORMATION (CARD HOLDER)												
1. Last Name Doe			First Name John			Init Q	2. Email Address					
3. Agency / Office / Division / Section / Unit												
4. Business Street Address					5. Business City			State		Zip		
6. Business Phone No.				Extension		7. Last 4 digits SS#		8. Birth Date (month & day only-mmdd)				
9. State User Access <input type="checkbox"/> State Employee <input type="checkbox"/> Contractor / Company Name							10. Vendor Access Vendor Company Name					
SECTION II – SERVICE REQUESTED												
1. Access Requested <input type="checkbox"/> SecurID Only <input type="checkbox"/> Dial-in <input type="checkbox"/> VPN If checked, VPN Group _____ <input type="checkbox"/> Both <input type="checkbox"/> User GW-toGW - RGWSUVPN <input type="checkbox"/> Vendor GW-to-GW - RGWVVPN Labor Units _____ Code _____ <u>NLROAM</u>												
2. Firewall Access requested: Destination, TCP/IP Port												
3. Change Access Type – Existing assigned token only Add: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN Remove: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN												
4. Reissue – No Division Approval required for reissue Reissue												
5. Cancel Token (Check appropriate reason) <input type="checkbox"/> Lost <input type="checkbox"/> Expired <input type="checkbox"/> No longer needed <input type="checkbox"/> Defective / Damaged						6. Token Serial # / Tunnel Name 12345678						
SECTION III – DIVISION APPROVAL												
1. Division Approver Name Lotsa Cash						2. Telephone Number (517) 555-5555						
3. Division Approver Signature MUST BE SIGNED						Date 01/01/05						
SECTION IV – DEPARTMENT SECURITY ADMINISTRATOR APPROVAL												
1. Security Administrator Name Iam D'Man						2. Telephone Number (517) 555-9876						
3. Security Administrator Approval Signature MUST BE SIGNED						Date 01/01/05						
SECTION V – BILLING INFORMATION												
1a. Ag Code XXX	1b. Index XXXX	1c. PCA XXXXX	1d. COBJ XXXX	1e. AOBJ XXXX	1f. Project # XXXX	1g. Prj Ph XXXX	1h. Grant # XXXX	1i. Grt Ph XXXX	1j. Ag 1 XXXX	1k. Ag 2 XXXX	1l. Ag 3 XXXX	
When the above information has been completed, fax this form to (517) 241-8016.												
HELP DESK USE ONLY												
1. Ticket Number			2. Assigned by:						3. Date			
NOC SECURITY USE ONLY – NEW CARD												
4. Token Serial #			5. SecurID Administrator Signature (Required)						6. Start Date			
NOC SECURITY USE ONLY – CANCEL CARD <i>Note: DIT will continue to charge Agency until card is returned or reported lost</i>												
7. Token Received by Signature						8. End Date						

3.3.5a Explanation of form information

Purpose: The proceeding form is used to change who is paying for a service. Dial-In, VPN, Both, and SecurID can be changed in this manner.

Specific field information:

SECTION I

Block(s) 1-10 = General user data. Only the name filed is required

SECTION II

Block(s) 1 - 5 = Not required

Block(s) 6 = Enter the token serial number

SECTION III

Block(s) All = This area must be completed by the individual or group in your agency that has been granted authority to expend the financial resources required to pay for the service. A signature is required or the form will be rejected by CSC.

SECTION IV

Block(s) All = This area must be completed by the individual or group in your agency that has been identified as the security authority for your agency by the enterprise security office. This person is often referred to as the *Authorized Requestor* and the list, maintained by OSDR, called *Authorized Requestor List by Agency and Category* may be obtained from that office. A signature is required or the form will be rejected by CSC.

SECTION V

Block(s) 1a – 11 = The new billing codes to be used to pay for the service. The minimum blocks are 1a through 1c but some agencies require additional blocks be completed. Please refer to Appendix I for specific agency requirements

The remainder of the form is used exclusively by DIT and need not be completed by agency personnel.

3.3.6 Reissue (replacement) of lost or expired token

REMOTE ACCESS SERVICE REQUEST
Michigan Department of Information Technology

SECTION I – EMPLOYEE INFORMATION (CARD HOLDER)												
1. Last Name Doe			First Name John			Init Q	2. Email Address					
3. Agency / Office / Division / Section / Unit												
4. Business Street Address					5. Business City			State		Zip		
6. Business Phone No.				Extension		7. Last 4 digits SS#			8. Birth Date (month & day only-mmdd)			
9. State User Access State Employee <input type="checkbox"/> Contractor / Company Name							10. Vendor Access Vendor Company Name					
SECTION II – SERVICE REQUESTED												
1. Access Requested <input type="checkbox"/> SecurID Only <input type="checkbox"/> Dial-in <input type="checkbox"/> VPN If checked, VPN Group _____ <input type="checkbox"/> Both <input type="checkbox"/> User GW-toGW - RGWSUVPN <input type="checkbox"/> Vendor GW-to-GW - RGWVVPN Labor Units _____ Code <u>NLROAM</u>												
2. Firewall Access requested: Destination, TCP/IP Port												
3. Change Access Type – Existing assigned token only Add: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN Remove: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN												
4. Reissue – No Division Approval required for reissue <input checked="" type="checkbox"/> Reissue												
5. Cancel Token (Check appropriate reason) <input checked="" type="checkbox"/> Lost <input checked="" type="checkbox"/> Expired <input checked="" type="checkbox"/> No longer needed <input checked="" type="checkbox"/> Defective / Damaged						6. Token Serial # / Tunnel Name 12345678						
SECTION III – DIVISION APPROVAL												
1. Division Approver Name Lotsa Cash						2. Telephone Number (517) 555-5555						
3. Division Approver Signature MUST BE SIGNED						Date 01/01/05						
SECTION IV – DEPARTMENT SECURITY ADMINISTRATOR APPROVAL												
1. Security Administrator Name Tam D'Mari						2. Telephone Number (517) 555-9876						
3. Security Administrator Approval Signature MUST BE SIGNED						Date 01/01/05						
SECTION V – BILLING INFORMATION												
1a. Ag Code XXX	1b. Index XXXX	1c. PCA XXXXX	1d. COBJ XXXX	1e. AOBJ XXXX	1f. Project # XXXX	1g. Prj Ph XXXX	1h. Grant # XXXX	1i. Grt Ph XXXX	1j. Ag 1 XXXX	1k. Ag 2 XXXX	1l. Ag 3 XXXX	
When the above information has been completed, fax this form to (517) 241-8016.												
HELP DESK USE ONLY												
1. Ticket Number			2. Assigned by:					3. Date				
NOC SECURITY USE ONLY – NEW CARD												
4. Token Serial #				5. SecurID Administrator Signature (Required)					6. Start Date			
NOC SECURITY USE ONLY – CANCEL CARD Note: DIT will continue to charge Agency until card is returned or reported lost												
7. Token Received by Signature							8. End Date					

3.3.6a Explanation of form information

Purpose: The proceeding form is used to replace a lost or expired SecurID token.

Specific field information:

SECTION I

Block(s) 1-10 = General user data. All fields must be complete.

SECTION II

Block(s) 1-3 = Not required

Block(s) 4 = Check the reissue box

Block(s) 5 and 6 = Check the reason for the cancellation(Lost or Expired) and enter the token serial number

SECTION III

Block(s) All = Not required.

SECTION IV

Block(s) All = This area must be completed by the individual or group in your agency that has been identified as the security authority for your agency by the enterprise security office. This person is often referred to as the *Authorized Requestor* and the list, maintained by OSD, called *Authorized Requestor List by Agency and Category* may be obtained from that office. A signature is required or the form will be rejected by CSC.

SECTION V

Block(s) 1a – 1l = The billing codes to be used to pay for the service. The minimum blocks are 1a through 1c but some agencies require additional blocks be completed. Please refer to Appendix I for specific agency requirements

The remainder of the form is used exclusively by DIT and need not be completed by agency personnel.

3.4 DIT-0051 Answers to Frequently Asked Questions (FAQ)

3.4.1 General

- A transfer requires two forms, a new service request and a canceled service request
- A reissue of a defective token requires two forms, a reissue and a canceled service request (this ensures the new token can be issued while the cancellation form and associated remedy case are held to track the return of the defective token)
- A reissue of a Lost or Expired token requires one form (this can be accomplished on one form because a case does not need to be opened to track the return of a lost or expired token)
- A reissue does not require Department Director or Security Administrator signatures
- Billing information shown is the absolute minimum required by DIT financial services. Additional information is required by several agencies. Appendix I illustrates required fields by agency
- A cancellation request is not processed until the physical SecurID token is received by the CSC. Billing will continue until the request is processed. Cancellation request with out tokens will be closed after 10 business days and the requestor will have to resubmit the DIT-0051.
- **DIT-0051s carried into, faxed to, or mailed to anywhere but the CSC will not be processed. It is imperative that the CSC be the only place that these forms are sent.**
- Dropping tokens off anywhere else besides the CSC is a bad idea. You will not get a receipt and no work or billing changes will be accomplished until the token is received by the CSC

3.4.2 Vendor specific

- Vendor VPN request require specific destination IP address and TCP/UDP port information.
- Vendor VPN accounts expire every 90 days and must be renewed by the authorized requestor prior to the expiration date to avoid service interruptions.

3.5 Picking up or dropping off SecurID tokens

SecurID requests are processed at the Client Service Center that is located on the third floor at Grand Tower on Grand Avenue downtown. Our address is

DIT
Client Service Center
235 S. Grand Ave., Suite 304
Lansing MI, 48909
(517) 241-9700
(800) 968-2644

When you enter the building proceed to the elevators. If you do not have a valid State of Michigan ID then check in at the guard desk just inside the door and tell her/him that you are here to pick up or drop off SecurID tokens. Exit off the elevator on the third floor and head West (or towards the street side of the building). Token pickup/drop off is located at Gloria Patterson's desk.

Here are a couple of points to remember about dropping off tokens:

1. A cancellation request is not processed until the physical SecurID token is received by the CSC. Billing will continue until the request is processed.
2. Cancellation request with out tokens will be closed after 10 business days and the requestor will have to resubmit the DIT-0051.
3. Tokens should not be dropped off anywhere but at the CSC. You will not get a receipt and no work or billing changes will be accomplished until the token is received by the CSC which you have no guarantee will happen.
4. The only thing that needs to be brought to the CSC when you return a SecurID token is the token itself and a case if one was provided. Please **DO NOT** bring print outs of Remedy tickets, Yellow stickies, copies of DIT-0051s, etc, as they are not required and will be discarded. A receipt for your tokens will be provided and signed at the drop off point. An envelope to hold several tokens would be appreciated.

3.5.1 Security check at pickup

When a SecurID request is processed and a delivery sheet is printed a 4 to 10 digit delivery key is randomly generated and printed at the bottom of the delivery sheet. This number is then copied into the Remedy ticket before the job is resolved. The authorized requestor will receive an email notification of the completion of the job with this number in the body of the message. Any individual can be sent to pickup the newly issued tokens but they must be given and provide the key to the person who distributes them at the CSC. This security check has been implemented to provide flexibility to the authorized requestors and preclude the need to maintain a list of authorized pickup agents and ID card checks at the CSC.

4.0 Remote access configurations (step by step)

4.1 SecurID (setting the PIN)

A new SecurID token is shipped in "New PIN mode". This means that the token cannot be used until the end user or a designated official creates a Personal Identification Number (PIN) that is associated with the token. There are two means by which a end user can set his/her own PIN. This section will cover those processes.

4.1.1 Dialing in via a modem

On Windows XP and Windows 2000

1. Insure that your computer has a modem installed and that it is properly connected to an operational phone line
2. Pick **Start/Programs/Accessories/Communications/HyperTerminal**
3. On the **Connection Description** Screen enter the name "*StateOfMichigan*" or something descriptive
4. On the **Connect to** screen type *371-8031* in the Phone number field
5. Click **OK**
6. On the **Connect** screen verify that the information is correct and click **Dial**
7. You will hear the modem dial and make the connection. After a few seconds a screen will pop-up with a **State Of Michigan** banner on it. On this screen the system is asking you to log in. Type your **Username** and hit *Enter*.
8. The next line is asking for your **PASSCODE**. Wait for the number to change and type the 6 digits into this field and hit *Enter*.
9. At the "**Do you want to enter your own pin?**" question type *y* and hit *Enter*.
10. At the "**Enter your new Numerical PIN, containing 4 to 8 digits**" prompt enter a number that you can remember that is at least 4 digits but not more than 8 digits in length and hit *Enter*.
11. At the "**Reenter PIN:**" prompt retype the same number again and hit *Enter*.
12. If you get the NOC_Dialin_1> prompt you have successfully set your PIN. Type *exit* and hit *Enter* to end your session.
13. Close HyperTerminal

On Windows NT

1. Insure that your computer has a modem installed and that it is properly connected to an operational phone line
2. Pick **Start/Programs/Accessories/HyperTerminal/HyperTerminal**
3. On the **Connection Description** Screen enter the name "*StateOfMichigan*" or something descriptive
4. On the **Connect to** screen type *371-8031* in the Phone number field
5. Click **OK**
6. On the **Connect** screen verify that the information is correct and click **Dial**
7. You will hear the modem dial and make the connection. After a few seconds a screen will pop-up with a **State Of Michigan** banner on it. On this screen the system is asking you to log in. Type your **Username** and hit *Enter*.
8. The next line is asking for your **PASSCODE**. Wait for the number to change and type the 6 digits into this field and hit *Enter*.
9. At the "**Do you want to enter your own pin?**" question type *y* and hit *Enter*.
10. At the "**Enter your new Numerical PIN, containing 4 to 8 digits**" prompt enter a number that you can remember that is at least 4 digits but not more than 8 digits in length and hit *Enter*.
11. At the "**Reenter PIN:**" prompt retype the same number again and hit *Enter*.
12. If you get the NOC_Dialin_1> prompt you have successfully set your PIN. Type *exit* and hit *Enter* to end your session.
13. Close HyperTerminal

4.1.2 Via the Internet

1. Insure that your computer is connected to the Internet
2. Open your web browser and point it to <https://websync.state.mi.us> and hit *Enter*.
3. At the “**RSA SecurID User Name and PASSCODE Request**” screen enter your *Username* in the **Username** files and the *currently displayed 6-digit number* on your SecurID token in the **PASSCODE** field.
4. Click “**Send**”
5. On the “**RSA SecurID New PIN Request**” screen insure that the “**I will create my PIN**” radio button is selected and type in *a 4 to 8 digit number* that you can remember in the “**New PIN:**” field. Verify your new PIN in the “**Verify New PIN:**” field and click **Send**.
6. You will be returned to the “**RSA SecurID User Name and PASSCODE Request**” page and your **Username** will be filled in. Type in your new *PASSCODE* which is your new PIN + the currently displayed 6-digit number on your SecurID token.
7. Click **Send**. You should now be re-directed to a screen that says:

CONGRATULATIONS!

You have been successfully authenticated into the State of Michigan networks. Your SecurID is working properly

4.2 Setting up Dial-In (Dialup networking)

4.2.1 On Windows XP

1. Start and login to your computer if it requires a login.
2. From the **Start** menu *pick Control Panel*
3. *Double click* on **Network Connections**
4. On the left side of the **Network Connections** window in the **Network Tasks** section *click Create a new connection*.
5. The **New Connection Wizard** will start *click “Next”*.
6. On the **Network Connection Type** screen choose “**Connect to the Network at my workplace**” by *clicking* on the radio button. *Click “Next”*.
7. On the **Network Connection** screen chose **Dial-up connection** from the list and *click “Next”*.
8. On the **Connection entry** screen type “*State of Michigan*” or something else descriptive and *click “Next”*.
9. On the **Phone number to dial** screen type in *371-8031* and *click “Next”*. You may have been given an alternate number for your location, if so, use it instead. If you need to dial a digit to get an outside line (such as 9) add it in front of the number followed by a comma (9,371-0831). If the 371 exchange isn’t in your local area add a 1 and the area code 517 (1-517-371-8031). You may need to add them all (9,1-517-371-8031).
10. On the **Connection availability** screen choose “**My use only**”. *Click “Next”*

11. On the **Completing the New Connection Wizard** screen *click* the check box next to **Add a shortcut to this connection to my desktop** and *click* **“Finish”**
12. A **Connect “State of Michigan”** (or whatever you called the connection in step 8) will pop up. Type in your *Username* and your *PASSCODE* and *click* **“Dial”**. It is best to wait until the SecurID token number has just changed before entering your *PASSCODE*.
13. A small information screen will pop up on the bottom right of your computer screen stating **“Connected to “State of Michigan””**. If you don't see this message see the troubleshooting section for help.
14. You are now logged in and may use your installed applications.

4.2.2 On Windows 2000

1. Start and login to your computer if it requires a login.
2. From the Start menu pick Settings/Control Panel
3. On the Control Panel double click Network and Dial-up Connections
4. From the Network and Dial-up connections screen double click Make New Connection icon
5. The Network connection wizard will start. Click **“Next”**
6. Pick Dial-Up to a private network from the list and click **“Next”**
7. On the **Phone number to dial** screen type in *371-8031* and *click* **“Next”**. You may have been given an alternate number for your location, if so, use it instead. If you need to dial a digit to get an outside line (such as 9) add it in front of the number followed by a comma (9,371-0831). If the 371 exchange isn't in your local area add a 1 and the area code 517 (1-517-371-8031). You may need to add them all (9,1-517-371-8031).
8. On the **Completing the New Connection Wizard** screen *click* the check box next to **Add a shortcut to this connection to my desktop** and *click* **“Finish”**
9. A **Connect Dial-up connection** (or whatever you called the connection in step 8) will pop up. Type in your *Username* and your *PASSCODE* and *click* **“Dial”**. It is best to wait until the SecurID token number has just changed before entering your *PASSCODE*.
10. A small information screen will pop up **“Connected to “Dial-up connection””**. If you don't see this message see the troubleshooting section for help.
11. Click **“OK”**
12. You are now logged in and may use your installed applications.

4.2.3 On Windows NT

1. Start and login to your computer if it requires a login.
2. From the Start menu pick Programs/Accessories/Dial-Up Networking
3. On the Dial-Up Networking window click **“New”**
4. On the **“New Phonebook Entry Wizard”** window in the **“Name the new phonebook entry”** field, type **“ConnectToSoM”** or something descriptive and click **“Next >”**

5. On the “Server” window check both the “I am calling the Internet” and the “Send my plain test password if that’s the only way to connect” and click “**Next >**”
6. On the “Phone Number” window type the number you were provided to connect to the State of Michigan. If you were not provided a number then see the list provided at the end of this section. Click “**Next >**”
7. On the “New Phonebook Entry Wizard” window click “**Finish**”
8. You are now returned to the “Dial-Up Networking” window with your new “Phonebook entry to dial” selected. Insure that the phone number in the “Phone number preview” field is correct and includes any additional numbers that you may need to dial to get an outside line. Click “**Dial**”
9. The “Connect to ConnectToSoM” window now appears. Type your username as provided with your SecurID in the “User name” field. In the “Password” field type your PIN and the six-digit number currently displayed on the SecurID token card. Note: It is best to wait until the numbers change to give the maximum amount of time for the login process to complete. Do not fill in the Domain information or click the save password check box. Click “**OK**”
10. The modem will dial the State of Michigan server and perform the login and registration of you computer on the network. Once this is complete the Dial-Up Networking window will minimize itself onto your task tray at the bottom right of your desktop.
11. You are now logged in and may use your installed applications.

NOTES:

Additional dial-in numbers by area are; Saginaw 989-758-1949, Dimondale 517-636-6001 and 517-636-6015, Lansing 517-371-8031 and 517-346-6433, Detroit 313-456-4799, Grand Rapids 616-356-0997 and in Charlotte 517-645-4166.

If reconfiguring a dialup connection that was previously defined for another system (i.e. FIA Shiva server) you will need to open the property sheet for the connection and change the authentication method from “Encrypted Passwords” to “Allow any means including clear text”. The nature of SecurID passwords, one time user only, means that clear text is just as safe as encrypted and causes less overhead.

4.3 Setting up the VPN client

The Virtual Private Network (VPN) service offered by the State of Michigan requires a separate application be installed on your machine called SoM VPN Dialer. The application is a Cisco product and replaces the IPSEC component of the Microsoft Windows XP and Windows 2000 operating systems. This software is provided to the authorized requestor not directly to the end user. It is the responsibility of the authorized requestor to distribute the package to the end users.

The interaction of this program with other programs on your computer cannot be predicted and may have adverse effects on your system. The Network Operations Center has tested this application extensively and found it to be stable and reliable on State of Michigan PCs. Installation on privately owned systems is at the discretion of the user and

the State of Michigan will accept no responsibility for systems adversely effected by the installation of this application.

The package comes in the form of a ZIP file and is normally emailed to the authorized requestor. In some cases these individuals are extracting the compressed files and burning a compact disk for distribution to their end users. Others are simply forwarding the ZIP file in email to the end user. How this is handled in your agency is completely up to the authorized requestor.

In all cases the VPN Dialer is pre-configured for the VPN group for the particular request. This means that the installation process is very straight forward on the supported platforms (Windows XP and Windows 2000).

4.3.1 Installing the VPN client on Windows XP/2000/NT

1. Obtain the install package from the authorized requestor or whoever has been designated to distribute the software in your agency.
2. If the package was distributed in a .ZIP format extract it to a temporary directory on your hard drive.
3. Locate the Setup.exe file that is associated with the installation of this product either on the CD or in the directory that you extracted the .ZIP file into.
4. Double click the Setup.exe file
5. You will see the State of Michigan VPN Client Setup screen and files will be installed on your system.
6. After several seconds (depending on the speed of your machine) the install shield wizard will complete and you will be presented with a reboot requestor. Insure that “Yes, I want to restart my computer now.” Is selected and click “Finish”.
7. Your computer will restart and the client is ready for use.

4.3.2 Logging in to the VPN

1. Insure that the steps for installing the VPN client have been completed and that your computer is connected to the Internet. The easiest way to test this is to open your web browser and go to your favorite web page. It should display normally.
2. Once you have determined that you are connected start the VPN dialer by picking Start/Programs/State of Michigan VPN Client/SoM VPN Dialer.
3. The Cisco VPN Dialer will pop up. Insure that the connection entry has a name in it and that the Host name or IP address of remote server is set to 167.240.254.60. Or 167.240.254.61 in the case of a VendorVPN.
4. Click Connect
5. User Authentication for “Group-Name” requestor will pop up. Type in your assigned username and PASSCODE (your securid PIN number plus the currently displayed 6 digits number on the securid token with no spaces or other characters) into the appropriate fields. Click “Connect”.

6. Some information will scroll by and your will be presented with a splash screen reminding you “All users must comply with the State of Michigan acceptable use policy...” Click “Continue”.
7. Everything will minimize down to your task tray (the lower right box on your desktop where the system clock is) and a small lock icon will be added to the tray.
8. At this point you are connected to the system and should be able to operate normally.
9. To disconnect from the system right click the lock icon and choose “Disconnect”.

4.3.3 VPN Notes

- While you are connected to the VPN you will have no Internet access or access to other systems on your local network (i.e. Network printers will not function).
- Only requested, approved, and configured destinations are reachable via the VPN
- Your PC must be configured to use the applications as if you are physically connected to the State of Michigan networks. GroupWise, DCDS, and Remedy need to be locally installed on your machine and configured just as they are at work.
- In order to reach the public Internet you must first disconnect from the VPN.

5.0 Troubleshooting

5.1 SecurID

Problem	Possible cause	Fix action
You were given a SecurID token but not provided a PIN.	Your PIN has not been set	Follow the instructions for SecurID (setting your PIN)
	Your PIN has been set by your administrator but was not passed along or has not yet arrived	Contact your Security administrator for further instructions
You were provided a SecurID and PIN but you get an error when logging in.	Your token is in “Next token code” mode	This can happen when your token has drifted in time from the server and needs to be resynchronized or if you have failed to login properly three times in a row. Follow the instructions to set your pin via the Internet. The system will prompt you for the next token code. Wait for the 6-digit number to change and enter only the 6 digits into the requestor. If

		you get the congratulations screen attempt your login again.
	Your PIN is wrong or you have forgotten it	Contact your Security administrator for further instructions
Your token is blinking, blank, displaying gibberish, or says prog.	Your token is defective	Contact your Security administrator for further instructions

5.2 Dial-In

Problem	Possible cause	Fix action
No dial tone	Your phone line is down	Contact your phone company
	Your phone line is not properly connected to your computer	Check the cabling and insure that everything is connected in accordance with your modems manufactures instructions.
	Your modem is defective	Replace your modem
Modem dials but there is no answer	The State of Michigan modem bank is down	Contact the CSC(Client Service Center) at 517-241-9700 or 800-968-2644 then choose the option the represents your agency, then option 1 for hardware and open a trouble ticket. You can also dial a different modem bank if you have the phone number for one
	All modems in the State of Michigan modem bank are busy	Wait and try again later
Modem dials, you get connected and authenticated but you get prematurely disconnected.	There is a problem with the modem bank or the phone line.	Contact the CSC(Client Service Center) at 517-241-9700 or 800-968-2644 then choose the option the represents your agency, then option 1 for hardware and open a trouble ticket. You can also dial a different modem bank if you have the phone number for one
You get connected but can't log in	SecurID or Username issue	See Troubleshooting SecurID

5.3 VPN

Problem	Possible cause	Fix action
You launch the VPN dialer and hit connect but get an error “Remote Peer No Longer Responding”	You are not connected to the Internet	Check your Internet connection or contact your Internet Service Provider. Attempt to ping the VPN gateway. From a command prompt type “ping 167.240.254.60” and hit enter. You should get a positive response.
	The IP address of the VPN server is wrong	Check your connection entry and insure that the IP address is 167.240.254.60 if you are a state use or 167.240.254.61 if you are a vendor.
	The client installation is wrong, faulty, or corrupted	Contact your Security administrator for further instructions
You get a login prompt and type in the information but the login prompt just pops back up.	SecurID problem	See Troubleshooting SecurID
You get a login prompt and type in the information and then a screen pops up that says enter next token code	SecurID is out of synchronization	Wait for the numbers to change on the token and enter them in without the PIN. This will re-synchronize your token
You get connected and logged in but then you can’t do anything	System configuration issue	Contact your Security administrator for further instructions

6.0 CSC(Client Service Center) Procedures

This section is intended to provide step-by-step procedures for helpdesk technicians to process remote access requests and to work Level I trouble issues. This section assumes an in-depth understanding of Remedy and access to key DIT/NOC resources.

6.1 Processing Requests

6.1.1 New/Change/Cancel

1. Insure that the DIT-0051 is complete as in the example form. It is not the CSC(Client Service Center) responsibility to insure the accuracy of the information.
 - a. If there is missing information reject the form back to the requestor and refer them to this document
2. Open a Remedy ticket and include only the required information from the form in the work log
3. Assign the new ticket to the DIT SC Service Remedy queue
4. Fill in the ticket number, assigned by, and date fields on the DIT-0051.
5. The DIT-0051 should be handled in accordance with CSC(Client Service Center) office procedures or destroyed if it is deemed unnecessary for helpdesk operations.

6.1.2 Transfer

1. Follow the procedures for New/Change/Cancel requests only insure that there are two forms. One to cancel and one for new service.

6.2 Working Problems

This section provides some basic guidelines for working SecurID problems. For security reasons we will not cover system information in this document. Login procedures and address information will be provided in On the Job Training (OJT) sessions instructed by NOC personnel when requested by CSC management

6.2.1 Re-synchronization

One of the most common problems that users have is a token has drifted from symbolization with the ACE server. A token that has drifted to far will not authenticate its user. The easiest way to fix this problem is to have the user fix it himself. Refer him to the SecurID troubleshooting section of this document. If for some reason this is impossible then follow these steps.

1. Open the RSA ACE Server client and login
2. From the User menu pick edit user
3. Type in the users last name and hit enter
4. One of two things will happen

- a. If she is the only user in the system with that last name you will be taken directly to the users information page
 - b. If there is more than one user with that last name then you will be presented a list of users. Pick the user from the list and click OK.
5. Once you are at the Edit User window single click the token serial number to highlight it.
 6. Click edit assigned token
 7. Click Resynchronize token
 8. The resynchronize token screen pops up and asks for the currently displayed 6-digit number. Ask for this number and enter it in the field and hit enter
 9. Next you need to wait for the token to change and enter the new set of numbers. Hit enter
 10. The message, "Token successfully resynchronized" confirms you did it right.

6.2.2 PIN Resets

This procedure is necessary when a user has forgotten his PIN. It is a potential security issue because if the real user has lost his token and the person on the phone is just someone who found it the system will treat him or her as the actual user once they have a new PIN. To combat this issue the CSC collects social engineering data on each user to verify who is on the phone. This information is kept in the SecurID tracking database and protected by access control lists on the system that houses that information. If the information is not available in the database (not all users have provided this information) then the problem user will have to be referred to their Security administrator for conformation. If you can positively identify the user by asking them to supply either the last 4 digits of their social security or the day and month of their birthday then proceed with this procedure.

1. Open the RSA ACE Server client and login
2. From the User menu pick edit user
3. Type in the users last name and hit enter
4. One of two things will happen
 - a. If she is the only user in the system with that last name you will be taken directly to the users information page
 - b. If there is more than one user with that last name then you will be presented a list of users. Pick the user from the list and click OK.
5. Once you are at the Edit User window single click the token serial number to highlight it.
6. Click edit assigned token
7. Click the "New PIN mode" check box and then "OK"
8. At this point the user must set a new pin number. Refer them or walk them through the SecurID section on setting a new PIN number

6.2.3 When that doesn't work

Open a trouble ticket and assign it to 2nd Level Support.

Appendix I

Billing code requirements for DIT-0051 by agency

DEPARTMENT	AGENCY INDEX	PCA	COMP AGENCY		PROJECT		GRANT	
			OBJECT	OJECT	PROJECT	PHASE	GRANT	PHASE
			3 Digits	5 Digits	5 Digits	4 Digits	4 Digits	6 Digits
					*	*	**	**
EXECUTIVE	011	XXXXX		XXXXX		XXXX		
MANAGEMENT AND BUDGET	071	XXXXX		XXXX		XXXX		
INFORMATION TECHNOLOGY	084	XXXXX		XXXX		XXXX		
MICH ECONOMIC DEVELOPMENT CORP	085	XXXXX	XXXXX			XXXX		
ATTORNEY GENERAL	111	XXXXX		XXXX		XXXX		
CIVIL RIGHTS	151	XXXXX		XXXX		XXXX		
CIVIL SERVICE	191	XXXXX		XXXX		XXXX		
DEPARTMENT OF STATE	231	XXXXX		XXXX		XXXX		
HISTORY ARTS AND LIBRARIES	251	XXXXX		XXXX				
MICH GAMING CONTROL BOARD	270	XXXXX		XXXX		XXXX		
TREASURY	271	XXXXX		XXXX		XXXX		
LOTTERY	275	XXXXX	XXXXX	XXXX				
EDUCATION	313	XXXXX				XXXX		
COMMUNITY HEALTH	391	XXXXX	XXXXX	XXXX		XXXX		
FAMILY INDEPENDENCE AGENCY	431	XXXXX	XXXXX	XXXX		XXXX		
DEPARTMENT OF CORRECTIONS	472	XXXXX	XXXXX	XXXX		XXXX		
MILITARY & VETERANS AFFAIRS	511	XXXXX	XXXXX	XXXX		XXXX		
STATE POLICE	551	XXXXX	XXXXX	XXXX				
TRANSPORTATION	591	XXXXX	XXXXX	XXXX		XXXX		
CIS	631	XXXXX		XXXX		XXXX		
DLEG	641	Xxxxx		Xxxx		Xxxx		
NATURAL RESOURCES	751	XXXXX	XXXXX	XXXX		XXXX		
ENVIRONMENTAL QUALITY	761	XXXXX	XXXXX	XXXX		XXXX		
DEPARTMENT OF AGRICULTURE	791	XXXXX		XXXX		XXXX		
MICH DEPARTMENT OF CAREER DEV	801	XXXXX	XXXXX			XXXX		
MDCD/EMPLOYMENT SERVICE AGENCY	802	XXXXX	XXXXX	XXXX		XXXX		
AUDITOR GENERAL	910	XXXXX		XXXX				
HOUSE OF REPRESENTATIVES	914	XXXXX		XXXX				
LEGISLATIVE SERVICE BUREAU	917	XXXXX		XXXX				
JUDICIAL	950	XXXXX		XXXX				

*A project # requires a phase #.

** A grant # requires a phase #.

Appendix II

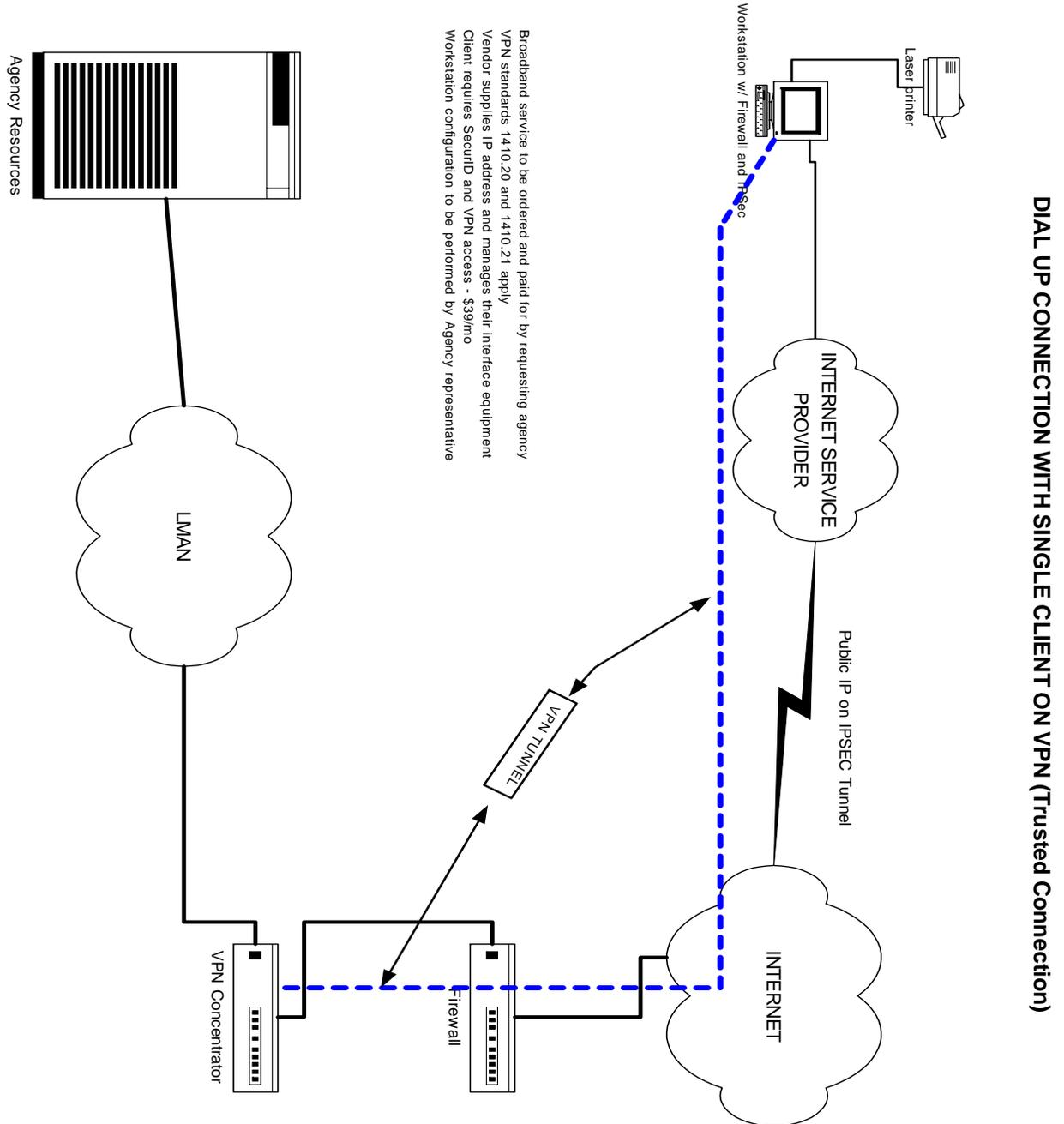
Remote Access Request Form DIT-0051

REMOTE ACCESS SERVICE REQUEST Michigan Department of Information Technology

SECTION I – EMPLOYEE INFORMATION (CARD HOLDER)												
1. Last Name				First Name				Init	2. Email Address			
3. Agency / Office / Division / Section / Unit												
4. Business Street Address						5. Business City			State		Zip	
6. Business Phone No. ()				Extension		7. Last 4 digits SS#		8. Birth Date (month & day only-mmdd)				
9. State User Access <input type="checkbox"/> State Employee <input type="checkbox"/> Contractor / Company Name								10. Vendor Access Vendor Company Name				
SECTION II – SERVICE REQUESTED												
1. Access Requested <input type="checkbox"/> SecurID Only <input type="checkbox"/> Dial-in <input type="checkbox"/> VPN If checked, VPN Group _____ <input type="checkbox"/> Both <input type="checkbox"/> User GW-toGW - RGWSUVPN <input type="checkbox"/> Vendor GW-to-GW - RGWVVPN Labor Units _____ Code _____ NLROAM												
2. Firewall Access requested: Destination, TCP/IP Port												
3. Change Access Type – Existing assigned token only Add: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN Remove: <input type="checkbox"/> Dial-in/ROAM <input type="checkbox"/> VPN												
4. Reissue – No Division Approval required for reissue <input type="checkbox"/> Reissue												
5. Cancel Token (Check appropriate reason) <input type="checkbox"/> Lost <input type="checkbox"/> Expired <input type="checkbox"/> No longer needed <input type="checkbox"/> Defective / Damaged								6. Token Serial # / Tunnel Name				
SECTION III – DIVISION APPROVAL												
1. Division Approver Name								2. Telephone Number ()				
3. Division Approver Signature								Date				
SECTION IV – DEPARTMENT SECURITY ADMINISTRATOR APPROVAL												
1. Security Administrator Name								2. Telephone Number ()				
3. Security Administrator Approval Signature								Date				
SECTION V – BILLING INFORMATION												
1a. Ag Code	1b. Index	1c. PCA	1d. COBJ	1e. AOBJ	1f. Project #	1g. Prj Ph	1h. Grant #	1i. Grt Ph	1j. Ag 1	1k. Ag 2	1l. Ag 3	
When the above information has been completed, fax this form to (517) 241-8016.												
HELP DESK USE ONLY												
1. Ticket Number				2. Assigned by:				3. Date				
NOC SECURITY USE ONLY – NEW CARD												
4. Token Serial #				5. SecurID Administrator Signature (Required)				6. Start Date				
NOC SECURITY USE ONLY – CANCEL CARD <i>Note: DIT will continue to charge Agency until card is returned or reported lost</i>												
7. Token Received by Signature								8. End Date				

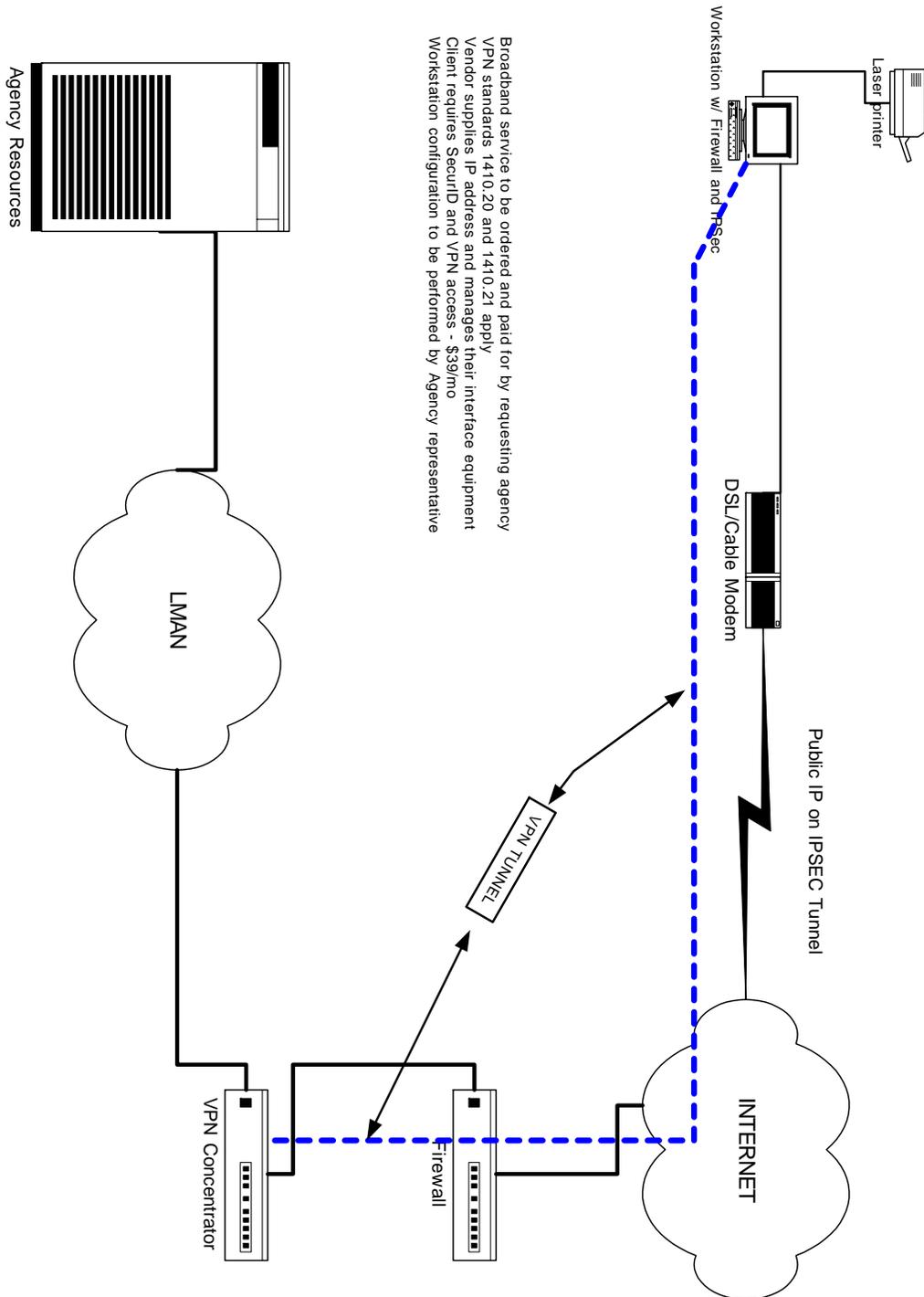
Appendix III

Dial Up Connection with VPN



Single User Broadband Connection

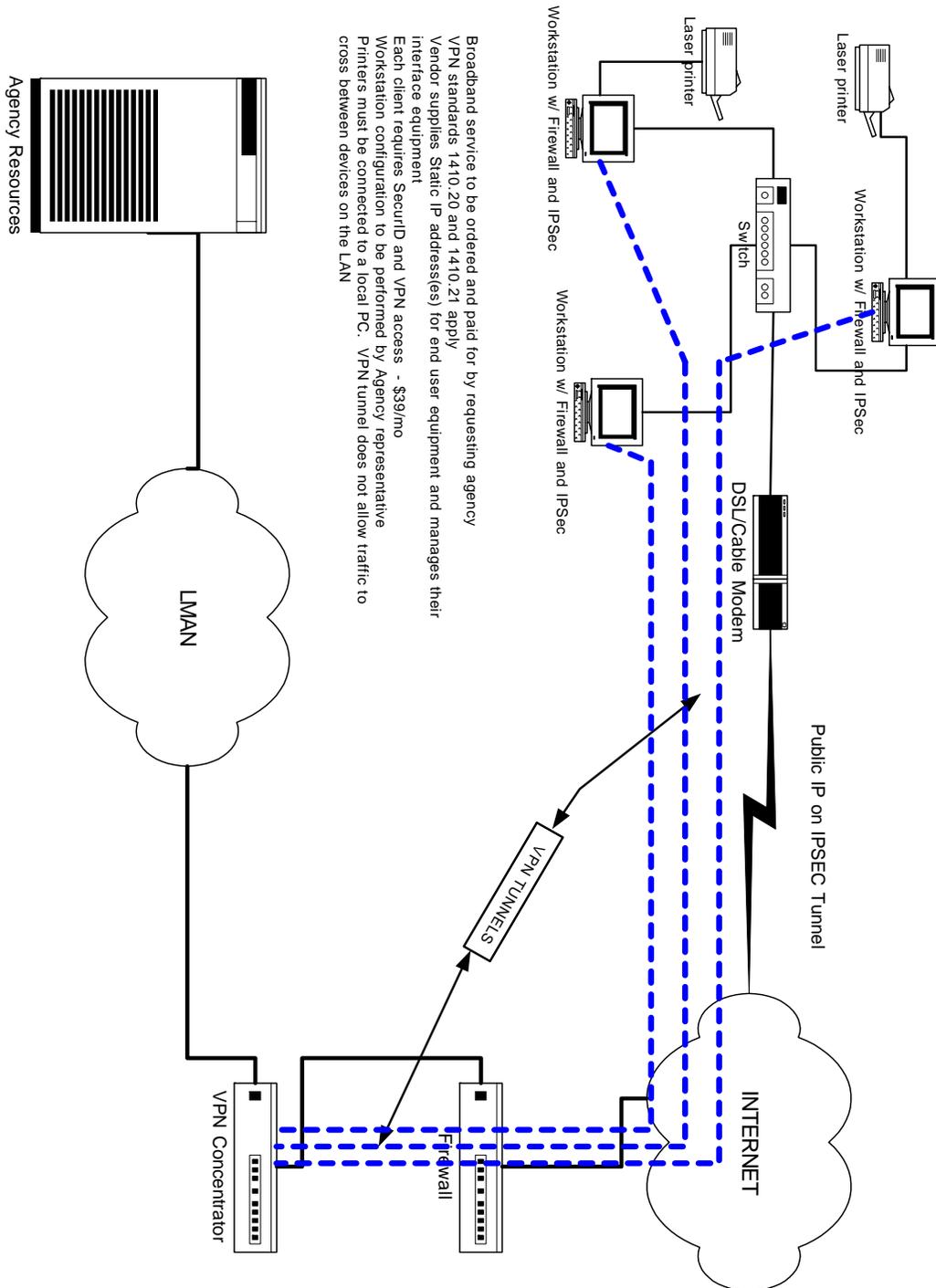
BROADBAND CONNECTION WITH SINGLE CLIENT ON VPN (Trusted Connection)



Broadband service to be ordered and paid for by requesting agency
VPN standards 1410.20 and 1410.21 apply
Vendor supplies IP address and manages their interface equipment
Client requires SecurID and VPN access - \$39/mo
Workstation configuration to be performed by Agency representative

Multiple User Broadband Connection

BROADBAND CONNECTION WITH MULTIPLE CLIENTS ON VPN (Trusted Connection)



Broadband service to be ordered and paid for by requesting agency
VPN standards 1410.20 and 1410.21 apply
Vendor supplies Static IP address(es) for end user equipment and manages their interface equipment
Each client requires SecurID and VPN access - \$39/mo
Workstation configuration to be performed by Agency representative
Printers must be connected to a local PC. VPN tunnel does not allow traffic to cross between devices on the LAN