ADAMS COUNTY

END USER REMOTE ACCESS SECURITY AGREEMENT

Name and Address of User**:**
End User
End User Address
City, ST Zip

This End User Access Security Agreement ("Agreement") is entered into by and between **End User** ("User"), and **Adams County**, ("Agency") and is effective as of May 14, 2003. This agreement outlines the terms and conditions under which Agency will provide Remote Access Security to User.

The VPN Service provides a secure means for User to access Agency data and/or networks via the public Internet. Data passing between User and Agency is encrypted while passing over the Internet.

1. Definitions

"Confidential Information" means information that may be used to distinguish, identify, or locate individual recipients of Agency's or the State of Washington's Services. Confidential Information may include, but is not limited to, addresses, Social Security numbers, email addresses, telephone numbers, financial profiles, credit card information, passwords, personal identification numbers, or lists of contacts.

"Digital Certificate" shall mean a unique digital identifier issued by a Washington State approved certificate authority, which is used to authenticate user and encrypt data.

"SecurID Token" shall mean a unique digital security appliance issued by a Washington State approved security token authority, which is used to authenticate user to a specific application.

"Proprietary Information" shall mean information that is of a sensitive and proprietary nature to Agency and its operations. Proprietary information may include, but is not limited to, passwords, Personal Identification Numbers (PIN), access codes, network security information, information relating to Agency's business affairs, employees, clients, finances, technology, software, source documents, data, or other information which User knows or has reason to know is of a sensitive or proprietary nature.

"VPN Service" shall mean the Virtual Private Network Service, administered and managed by the Department of Information Services. This VPN Service is a secured, remote access service provided to User.

2. Term

A. This Agreement shall stay in affect until the User's access to the VPN Service is terminated. Should the User come in contact with Confidential or Proprietary Information, the term of this Agreement shall extend until **two (2) years** after the VPN Service is terminated.

3. Agency Requirements

A. Subject to payment of applicable VPN Service fees, Agency will comply with State Information Technology Policies and Standards to provide the VPN Service to User. VPN Service will be provided pursuant to the terms and subject to the conditions contained in this Agreement.

B. Agency may, in it's sole discretion, elect to discontinue the VPN Service at any time.

C. Agency acknowledges and understands the provision of VPN Service is dependent on third-party providers. Agency shall not be held liable for actions or inactions of such third-party providers.

4. User Requirements.

A. Security Authentication Appliance

In order to receive VPN Service, the User may be required to obtain a SecurID token or a Digital Certificate. Should a SecurID token be employed in the VPN Service, the User will be solely responsible for the cost for lost or damaged SecurID tokens. Should a Digital Certificate be employed in the VPN Service, the User is solely responsible for obtaining a valid high assurance Digital Certificate. The cost to purchase a Digital Certificate is the sole responsibility of the User.

B. Software

User agrees to comply with the terms and conditions of all end user license agreements accompanying any software, SecurID tokens, or digital certificates distributed in connection with the VPN Service. The VPN Client software license is presented to User during the initial steps of the software installation.

C. Internet Access

User is required to maintain an account with an Internet Service Provider (ISP). The ISP connection will enable the User to connect to the VPN Service.

D. Equipment

User understands that the VPN Services requires an Intel Pentium or compatible Personal Computer, running Microsoft Windows 95, 98 NT 4.x, 2000 Workstation, or XP Professional. User is responsible for obtaining, configuring and maintaining compatible equipment.

E. Virus Protection Software

User is responsible for ensuring comprehensive virus protection software, including upgrades and patches consistent with industry standards, is implemented and maintained on the User's remote workstation.

F. Personal Firewalls

User is responsible for ensuring a comprehensive firewall, including upgrades, patches, and current versions consistent with industry standards, is implemented and maintained on the User's remote workstation.

5. Prohibited Uses

User agrees to refrain from the following prohibited uses:

A. Use of the VPN Service for any unlawful purpose.

B. Transmission of any content that is obscene pornographic, libelous, invasive of privacy rights, or advocates violence, bigotry, or bias based on race, color, religion, ancestry, national origin, gender orientation, or physical or mental disability.

C. Accessing any data and/or networks to which user does not have prior authorization to access.

D. Altering, tampering, or otherwise modifying the VPN Service, or the Software or Agency equipment used to provide the VPN Service.

E. Providing access to the VPN Service for others not affiliated with User.

F. Use of the VPN Service for means other than performing a purpose reasonably related to Agency's business.

G. Impersonate any person or entity, including, but not limited to, an Agency or Washington State official, falsely state or otherwise misrepresent your affiliation with an Agency or the State of Washington.

H. Modify, publish, transmit, transfer or sell, reproduce, create derivative works from, distribute, perform, link, display or in any way exploit any content from any Agency database.

I. Use or attempted use of the VPN Service after termination of this Agreement.

J. Upload, post, email, otherwise transmit, or post links to any material that contains software viruses, worms, Trojan horses, time bombs, trap doors or any other computer code, files or programs or repetitive requests for information designed to interrupt, destroy or limit the functionality of any Agency computer software or hardware, telecommunications equipment, or Agency data or to diminish the quality of, interfere with the performance of, or impair the functionality of the VPN Service.

K. Use of the VPN Service to connect a LAN or other network to Agency's network.

6. Treatment of Confidential and Proprietary information.

A. User acknowledges that some of the material and information which may come into it’s possession or knowledge in connection with User's use of the VPN Service, may be Confidential Information or Proprietary Information. User agrees to hold all such Confidential Information or Proprietary Information in strictest confidence and not to make any use of such Confidential Information or Proprietary Information for any purpose other than an Agency-related business purpose, to release it only to authorized employees or subcontractors requiring such Confidential Information or Proprietary Information for the purposes of carrying out the Agency-related business purpose, and not to release or disclose it to any other party. User agrees to release such Confidential Information or material only to employees or subcontractors who have signed a written non-disclosure agreement, expressly prohibiting disclosure. User agrees to implement physical, electronic, and managerial safeguards to prevent unauthorized access to Confidential Information or Proprietary Information. Immediately upon termination of this Agreement, User shall certify to Purchaser the destruction or return of all Confidential Information or Proprietary Information to Agency.

B. This Section does not impose any obligation on the User, if the Confidential Information or Proprietary Information is:

1. (a) publicly known at the time of disclosure;
2. (b) already known to the receiving party at the time;
3. (c) furnished by Agency or Purchaser to others without restrictions on its use or disclosure;
4. (d) independently developed by the receiving party without use of the confidential information

C. Except for its own internal use in carrying out a legitimate Agency-related business purpose, User

agrees not to collect, store, sell or distribute any Confidential Information or Proprietary Information collected or derived from its use of the VPN Service

D. Violation of this section by User may result in immediate termination of this Agreement, monetary damages, or statutory penalties.

7. Indemnification

User agrees to promptly defend and indemnify, and to hold harmless from, against and in respect of, and pay or reimburse for, any and all claims, demands, liabilities, losses, damages, costs and expenses, including reasonable attorneys' fees, of the Agency, its employees, and other Users, arising from, relating to or in connection with an alleged or actual breach by User of User's obligations under this Agreement. User further agrees to cooperate fully with Agency and legal counsel in resolving any claim or dispute.

8. Blocking of VPN Service

User acknowledges that Agency or its third-party providers shall have the right to block User's access to the VPN Service, in whole or in part, at any time, for any reason.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed as of the date first above written.

End User		**Adams County**	
Signature:	_____	Signature:	_____
Title:	_____	Title:	_____
Date:	_____	Date	_____