INTERNET ACCESS REQUEST AND AGREEMENT

Internet access and services are provided for official DSHS business activities. The integrity of DSHS and the protection of its information and clients are dependent on the professional and ethical conduct by all DSHS representatives using Internet resources. Some Internet activities are illegal or inappropriate and, therefore, are unauthorized. Many of the listed unauthorized activities are compiled from other DSHS policies and state regulations, and are identified here for convenience of review. The unauthorized activities include, but are not limited to, the following:

1. Introducing computer viruses or other destructive programs into DSHS and/or external systems or networks via the Internet.

2. Intercepting and decrypting traffic transmitted over the Internet that belongs to others, except as part of an official investigation. (Decrypting is the process of unscrambling the characters in encrypted text to make the data readable. Encryption is the art and science of keeping messages secure by scrambling the text to make them unreadable except by the intended recipient. Cryptographic keys are used to encrypt and decrypt messages.)

3. Packet sniffing for other than official network trouble-shooting procedures. (Packet sniffing is a term used for intercepting and reading the unencrypted text of packets transmitted over the Internet.)

4. Packet spoofing. (Packet spoofing is a term used to identify methods of gaining unauthorized access to a computing system or network.)

5. Infringing on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.

6. Violating any local, state, national, or international law, including U.S. exports control laws and regulations (e.g., transmitting an encryption algorithm with keys greater than 40 bits to a foreign country).

7. Transmitting political material.

8. Transmitting information and/or materials of a personal nature, or transmitting advertising or commercial materials for personal benefit. Per division policy, occasional use of e-mail may be permitted if it does not interfere with an employee's normal job responsibilities and does not result in additional cost to the state.

9. Flaming. (**Flaming** is the use of derogatory comments during Internet communication.)

10. Bombing. (**Bombing** is the act of repeatedly sending an identical message to a particular address.)

11. Spamming. (**Spamming** is a variant of **bombing**; it refers to sending e-mail to hundreds or thousands of users or to lists that expand to that many users.)

12. Using hypertext to point or link DSHS web sites to other Internet/World Wide Web (WWW) sites whose content may be in violation of the mission or policies of DSHS. (Hypertext is any text that contains links to other documents [words or phrases in the document that can be chosen by a reader], and which causes another document to be retrieved and displayed.)

13. Creating, posting, transmitting, or voluntarily receiving:

    a. Obscene or pornographic material (except for official DSHS investigative activities);
    b. Offensive, libelous, threatening, or harassing material; and
    c. Degrading statements based on race, national origin, gender, sexual orientation, age, disability, and religious or political beliefs.

14. Ordering or selling items or services on the Internet, except as specifically approved by DSHS for business purposes.

15. Gambling.

16. Participating in any on-line contest or promotion.

17. Accepting promotional or other gifts.

18. Playing or downloading games. (Downloading is transferring a file from an Internet site to a computer.)

19. Participating in non-business related chat/forum groups, list servers, or newsgroups. (Chat/forum groups are real-time discussion groups that allow users to communicate interactively. List servers are mailing list programs for group communication. Newsgroups are Internet-based bulletin boards facilitating the posting/reading of messages along a given topic.)

20. Sending/forwarding chain letters.

21. Soliciting money for religious or political causes, or for non-DSHS events.

22. Unauthorized accessing of protected government information or resources.

INTERNET ACCESS REQUEST AND AGREEMENT

To use or obtain Internet access, the requester must first read, complete, sign, obtain signatures, and forward this form as identified by the division policy.

Requester's Name: ______________________________ Phone #: __________

Organization: ______________________________

Manager's Name: ______________________________ Phone #: __________

Business justification for requested access (why you need access to the Internet):

E-mail and World Wide Web are automatically provided.
Additional Internet access required:

________ Export FTP (File Transfer)

________ Telnet (Sign-on) IP Address to connect

Organization Name:

Special Requirements:

________ Installation of a File Browser (Gopher) (Please Specify):
________ Other (Please Specify):

STATEMENT OF AGREEMENT

I have read the DSHS Internet policy and the list of unauthorized Internet activities on this form. I understand that Internet access and services are being provided for me to use in my current position/work assignment only. I agree to comply with all related DSHS and division policies, and specifically this form and Administrative Policy 15.14, Internet Use and Connectivity. I understand that any activity that occurs through this Internet access may be monitored. I also understand that failure to comply with the established policies can result in the loss of my DSHS-provided Internet access and services, and could lead to disciplinary action.

Requester's Signature: ______________________________ Date: ______

Requester's Manager's Signature: ______________________________ Date: ______

Approved by: ______________________________ Date: ______
(organization designee, if required)