Department of Finance
Acceptable Use Policy

1.0 Overview
Department of Finance Cyber Security Team intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Department of Finance's established culture of openness, trust and integrity. Department of Finance Cyber Security Team is committed to protecting Department of Finance's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Department of Finance. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review ***Human Resources policies*** for further details.

Effective security is a team effort involving the participation and support of every Department of Finance employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose
The purpose of this policy is to outline the acceptable use of computer equipment at Department of Finance. These rules are in place to protect the employee and Department of Finance. Inappropriate use exposes Department of Finance to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other workers at Department of Finance, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Department of Finance.

4.0 Policy
4.1 General Use and Ownership

1. While Department of Finance's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the government systems remains the property of Department of Finance. Because of the need to protect Department of Finance's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Department of Finance.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual divisions are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor, manager or director.

3. Division of Electronic Data Processing recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Department of Finance Information Sensitivity Policy. For guidelines on encrypting email and documents, go to ***Department of Finance Awareness Initiative***.

4. For security and network maintenance purposes, authorized individuals within Department of Finance may monitor equipment, systems and network traffic at any time, per Department of Finance Audit Policy.

5. Department of Finance reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by government confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, government strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six (6) months.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.

4. Use encryption of information in compliance with ***Department of Finance Acceptable Encryption Use policy***.

5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the ***"Laptop Security Tips".***

6. Postings by employees from a Department of Finance email address to newsgroups should contain a *disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Department of Finance, unless posting is in the course of business duties*.

7. All hosts used by the employee that are connected to the Department of Finance Internet/Intranet/Extranet, whether owned by the employee or Department of Finance, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or governmental policy.

8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. *If you suspect anything, contact the Department of Finance Cyber Security Team immediately.*

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of Department of Finance authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Department of Finance-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Department of Finance.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Department of Finance or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a Department of Finance computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any Department of Finance account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to Division of Electronic Data Processing is made.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal or printer session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, Department of Finance employees to parties outside Department of Finance.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within Department of Finance's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Department of Finance or connected via Department of Finance's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.

ATTENTION: READ THE FOLLOWING CAREFULLY BEFORE SIGNING DOCUMENT

I, _____ on this day _____/_____/_____ confirm that I have
Print Name (first, middle initial, last) *mm dd yyyy*
read, understood and have accepted the terms of the Department of Finance's "Acceptable Use Policy". I am fully aware that I will be held accountable for any violation of the EDP "Acceptable Use Policy".

Full Name:_____
Print
Department:_____
Print
Division:_____
Print
Job Title:_____
Print
Contact#:_____

Email address: _____

Signature of Applicant:_____ Date:_____/_____/_____

Witnessed by:_____ Date:_____/_____/_____
Print