



INTERNET / INTRANET

ACCEPTABLE

USE

POLICY

Government of Antigua & Barbuda
Internet / Intranet Acceptable Use Policy

PART I	PAGE
<u>Introduction</u>	3
<u>Scope</u>	3
<u>Policy Updates</u>	3
<u>User Awareness</u>	4
<u>Provision of Service</u>	4
<u>Personal Use of Internet</u>	5
<u>Prohibited Uses</u>	5-6
<u>Exceptions to Prohibited Use</u>	6
<u>Monitoring</u>	7
<u>Unintentional Incidents</u>	7
<u>Uploading and Downloading of Files</u>	7
<u>Newsgroups</u>	8
<u>Email and Newsgroups Use Policy</u>	8-10
<u>Publication of Material</u>	10
<u>Breach of Policy</u>	10-11
<u>Further Information</u>	11
<u>History</u>	11
 PART II	
<u>Enforcing The Acceptable Use Policy</u>	12
<u>Introduction</u>	13
<u>Background</u>	13-14
<u>Proposed Solution</u>	14
<u>Hardware</u>	14
<u>Software and User Access</u>	14-15
<u>Benefits</u>	15

1 Introduction

- 1.1 The Internet is a worldwide communication network linking together thousands of computer networks and many millions of users through public and private telecommunication lines.
- 1.2 The Government of Antigua and Barbuda (“GOAB”) provides access to the vast information resources and facilities of the Internet to help public sector workers and others do their jobs more efficiently and effectively. Such facilities include researching particular products, electronically communicating with colleagues and business associates and accessing central government data.
- 1.3 The facilities to provide that access represent a considerable commitment of government resources in respect of telecommunications, networking, security, software and support as well as significant costs. They also represent a significant risk if they are not used correctly.
- 1.4 This policy document is intended to define in a clear and straightforward manner what those risks are and the conditions under which the Internet and Intranet services might be used.

2 Scope

- 2.1 This policy applies to employees, members and all other users of the Government’s Internet services.
- 2.2 The policy applies equally to the Government’s internal version of the Internet, the Intranet, which uses similar technologies and poses similar risks. For ease of reading, the term Internet is used to refer to both services throughout the remainder of this document.

3 Policy Updates

- 3.1 This policy will be amended from time to time in response to changing circumstances as Internet facilities develop and in response to operational and legislative requirements.
- 3.2 The Government will do its best to ensure that individual users are made aware of these changes when they occur.
- 3.3 The most current version of the policy will, however, always be available on the Government’s Intranet site and in paper form from the Information Technology Center. As a condition of use, it is the responsibility of users to ensure that they keep up-to-date with the latest requirements of the policy.

4 User Awareness

- 4.1 All Internet users will be required to sign the following statement before being allowed access to the Internet:

I have read the Government's Internet / Intranet Acceptable Use Policy and fully understand the terms and conditions and agree to abide by them.

I understand that the Government's security systems will record for management use all Internet activity undertaken by me, including the addresses of web sites visited or attempted to be visited and any material transmitted or received.

I understand that violation of this policy may lead to disciplinary action, including termination of employment, and could also lead to personal criminal prosecution.

5 Provision of Service

- 5.1 The Government will provide Internet access to all staff who have signed the Acceptable Usage Policy where this is reasonably practicable.
- 5.2 The Government does, however, reserve the right to withdraw this facility at the request of service managers and in the event that the facility becomes uneconomic or is being abused.
- 5.3 Users must ensure that they use the facility lawfully at all times.
- 5.4 As a general policy, Internet access will only be made available through the Government's data network. There are several reasons for this:
- 5.4.1 The Government uses a fixed link to connect to the Internet and its charges are, therefore, fixed and predictable irrespective of usage level.
- 5.4.2 The Government can monitor usage levels and increase bandwidth as required to ensure an appropriate quality of service for all users at the most economic rates.
- 5.4.3 The Government can route all traffic through its firewalls and other security systems to protect users and the Government from inappropriate material.
- 5.5 Internet connections from stand alone personal computers (PCs) via broadband connections to private companies will only be permitted under very special circumstances and must be approved in writing annually by the Minister with responsibility for Information Technology or the Director of the Information Technology Center (IT Center). The user is responsible for obtaining and keeping this permission up-to-date.

5.6 Modem connections from networked workstations (including dual boot connections) to any other networks are specifically prohibited.

6 Personal Use of Internet

6.1 The Government's Internet facility is intended to support the organization's legitimate business requirements.

6.2 Occasional and reasonable use of the Internet for personal purposes is regarded as acceptable provided that:

6.2.1 Systems are not used for personal use during normal working hours.

6.2.2 Systems are not used for private business or other commercial purposes including the sale or purchase of goods and services.

6.2.3 Use of the system does not interfere with the normal performance of the user's duties.

6.2.4 There is no additional cost to the Government in using the system for personal use.

6.2.5 There is no breach of the prohibitions identified in this policy.

6.3 For the purposes of clarity, the Government connects to the Internet through a dedicated leased line at fixed costs. The costs to the Government, therefore, remain the same irrespective of the amount of use although performance levels will decline as the line reaches capacity.

6.4 The sites within the Government complex connect to the leased line directly and, therefore, no additional costs are incurred for personal use for persons working within the Government complex.

7 Prohibited Uses

7.1 The Government's Internet services may not be used for the transmitting, retrieving or storing of any communications or images, which are:

7.1.1 harassing - harassment is unwanted conduct (including insults and "jokes"), which relates to gender, race, sexual orientation, religion, disability or other similar issues.

7.1.2 defamatory - defamation is the publication of material, which adversely affects the reputation of a person, department or company.

7.1.3 copyright - copyright means that the owner of such material has the exclusive

right to determine how that material might be copied and used. Copyright material may not be transmitted if the owner's permission has not been obtained.

- 7.1.4 pornographic - pornographic means any material of a sexual nature. As there can be no possible legitimate business use for accessing or transmitting sexually explicit materials at work, the question of whether or not such material constitutes pornography is not relevant to the use of the Government's Internet services and all such material is prohibited.
- 7.2 Use of the Government's Internet facilities to deliberately propagate computer viruses, worms, Trojan horses or trap door programs is prohibited.
- 7.3 Use of the Government's Internet facilities to disable or overload any computer system or network, or to attempt to disable, defeat or circumvent any system intended to protect the privacy or security of another user is prohibited.
- 7.4 Users must not install additional Internet or email related software, or change the configuration of existing software without the written authorization of the Government's Director of the Information Technology Center.
- 7.5 Use of the Government's Internet facilities to download or distribute pirated software or data is prohibited.
- 7.6 Use of the Government's Internet facilities to upload software licensed to the Government, or to upload data owned by the Government without valid, written authorization, is prohibited.
- 7.7 Use of the Government's Internet facilities to download entertainment software of games or to play games over the Internet is prohibited.

8 Exceptions to Prohibited Use

- 8.1 Employees who have to monitor offensive materials as part of their jobs, (e.g. Child Protection, Trading Standards, etc) may access relevant material with their Head of Department's written permission.
- 8.2 Permission will only be given to named individuals and a record of such permissions must be placed on official file and copied to the Director of the Information Technology Center.
- 8.3 Each site visit made for such purposes must be recorded in a log, which identifies the site, the date and time of the visit and the purpose. The log must be retained for a minimum of two years from the date of the visit.

9 Monitoring

- 9.1 The Government uses special hardware and software to monitor and control the use of the Internet, which enables it to record (and if necessary view) all usage of the Internet. This includes, but is not limited to, user details, pages attempted, pages accessed, files downloaded, graphic images viewed and all email correspondence.
- 9.2 Users should not expect the use of the Internet or the contents of files to be private. All usage will be monitored, logged and retained as required to ensure that users are complying with the requirements of this policy and that no misuse is taking place.

10 Unintentional Incidents

- 10.1 The nature of the Internet is such that it may not always be possible to avoid accessing material, which is prohibited by the terms of this Acceptable Use Policy.
- 10.2 Users who are placed in this position should contact their Departmental IT support staff immediately so that their systems can be cleaned. If the departmental IT staff cannot clean the system, contact should be made with the IT Center's Help Desk at 481-5300. Accidental access will not result in disciplinary action but failure to report it may result in appropriate disciplinary action.
- 10.3 Users who believe that the Internet systems are being used in a way which they regard as being offensive, potentially illegal or which otherwise appears to contravene acceptable Government policy or statutory requirement should contact the Information Technology Center at 481-5300 or via e-mail support@antigua.gov.ag

11 Uploading and Downloading of Files

- 11.1 A significant benefit of the Internet is the ability to access and distribute files quickly and easily, and the Government is keen to ensure that this facility is available to users.
- 11.2 The Internet security systems implemented by the Government includes virus scanning software which is designed to intercept any viruses in files (including email attachments) and all files sent and received will be scanned.
- 11.3 Any incidents regarding the detection of viruses in files uploaded and downloaded using the Internet services will be logged and appropriate action taken by the Government's Director of the Information Technology Center.

12 Newsgroups

- 12.1 Newsgroups offer a wealth of potentially valuable information and advice but can also consume inappropriately large amounts of time and energy. In addition, newsgroup messages often provide links to inappropriate web pages and users should be aware of the risk of inadvertently accessing unacceptable sites by this means.
- 12.2 Users may only access newsgroups if so doing represents a reasonable return in terms of effort involved for the value received.
- 12.3 Users must not access newsgroups, which are not work related.
- 12.4 Users must not participate in discussions, which are politically sensitive or controversial, whether nationally or locally, and users must not give advice or information, which they know to be contrary to the Government's policies or interests.
- 12.5 Newsgroups are by definition public forums. Users must therefore not reveal any information, which might reasonably be deemed to be sensitive or confidential.

13 Email and Newsgroups Usage Policy

- 13.1 The use of office email address (your.name@antigua.gov.ag) is limited to government business only. Do not give out your office email address to any person or organization for personal contact. For personal contact, you may use hotmail or something else, but not your office email address.
- 13.2 Do not post your office email address anywhere on any website. You run the risk of getting more junk email that way. Also be careful about placing your office email in online directories if, for example, you are subscribing to newsgroups (or publications) for office purposes.
- 13.3 Before subscribing to a newsgroup for office purposes you are required to consult with your department's technology personnel or the Government Information Technology Center.
- 13.4 Do not use your office email to register for prizes or sweepstakes and NEVER end unsolicited email ("spam") for advertising or promotion of any sort.
- 13.5 Do not send attachments externally to anyone unless you have their permission to do so and do not send attachments that are larger than the recipients' mailbox can accept.

- 13.6 Do not allow others to send you attachments totaling more than six megabytes (6 MB) in size at any one time. Also, make sure that you clean out and archive your mailbox contents on a regular basis to ensure that your mailbox does not get filled up, and that there is a backup record of ALL official government emails.
- 13.7 Save all of your email attachments and do not practice the storage of the attachment within your email. If you have large files to transfer to anyone consult your Ministry's technology department or the Government Information Technology Center.
- 13.8 Never open suspicious or unexpected email attachments. They may contain a script or program that can delete your computer files, or create other severe damage within the network.
- 13.9 Please remember that email must follow the code of conduct as expected in any other form of written or face-to-face communication:
- DON'T configure personal web-based email (e.g. hotmail, yahoo mail) to automatically forward to work e-mail accounts (or vice versa).
 - DON'T forward restricted or confidential work email to your personal web-based e-mail account.
 - Almost no personal web-based email system provides encryption, security or privacy. Therefore, business information, information of a confidential or sensitive nature, such as credit card numbers, passwords and other personal information, should not be sent using ANY web-based email system.
 - NEVER open suspicious or unexpected email attachments. They may contain a script or executable program that can delete local files, send files/documents or passwords to another host and severely damage the network.
 - Passwords MUST not be words found in the dictionary.
 - Passwords MUST contain alpha and numeric characters and be at least 8 characters long.
 - Personal web-based email account passwords MUST not be the same as official department email account passwords.
 - Employees must not attempt to read another person's email unless otherwise authorized. Employees should have no reasonable expectation of privacy in email transmitted, received and stored on and/or through the government's system. Any email sent or received through the government's system is the property of the Government of Antigua and Barbuda and is not a private employee communication (whether created or received).
 - It is unacceptable to send large files such as singing Christmas cards or animated Valentine's greetings as attachments to email - such attachments can seriously affect the performance of a department's network. Remember that email is the leading source of computer viruses; be especially suspicious of attachments. Unencrypted email is not secure or private. Employees have

a responsibility to put only non-sensitive information in an email. The recipient is responsible for handling the message with respect and securing the sender's permission before forwarding it.

- Employees must have their head of department's permission before using the Government's Information Technology resources for large-scale distribution of e-mail.

13.10 Email that is of a personal or transitory nature need not be archived. However, email that is an official record of government is to be retained. Email is an official record if:

- It was created or received as part of the normal business practices of the department and it relates to the department's mandate,
- It documents, interprets or otherwise supports departmental policies, decisions, transactions and events or it contains informational value of significance to the department.

13.11 Many employees access personal or (other) work email through personal web-based accounts hosted on sites such as Hotmail or Yahoo. Currently, this incidental use of the Government's Information Technology infrastructure is permitted. However, such web-based email systems must be used cautiously. If irresponsible use of web-based email damages departmental computers and networks, permission to access personal web-based email from work may have to be rescinded.

14 Publication of Material

14.1 The Government has a corporate web site providing information about all of its services.

14.2 Because of the risks associated with the Internet and the need for the Government to maintain the clarity, consistency and integrity of its image, no user, section or directorate of the Government may establish or maintain a separate Internet or FTP site except where this is specifically authorized in writing.

14.3 Authorization for separate websites will only be given in exceptional circumstances and must be renewed annually. Authorization can ONLY be obtained through the Minister of Information Technology or the Director of the Government Information Technology Center and the user is responsible for obtaining and keeping this permission up-to-date.

15 Breach of Policy

15.1 This Acceptable Use Policy has been drafted in such a way as to protect both the Government and users and any breach of policy will be dealt with in accordance with the Government's general disciplinary procedures.

- 15.2 Failure to adhere to this policy will be considered to be a potentially serious disciplinary offence, which could lead to dismissal.
- 15.3 In addition, users are advised that the following actions may also be taken by third parties:
 - 15.3.1 Harassment is a criminal offence for which the harasser can be imprisoned. Victims of harassment may also be able to claim damages from the harasser as well as the Government.
 - 15.3.2 A person or company may sue individuals as well as the Government for damages if defamation of reputation can be demonstrated.
 - 15.3.3 A copyright owner may sue individuals for damages as well as the Government in the event of breach of copyright.
 - 15.3.4 Accessing and transmitting sexual material may be a criminal offence. The courts may take action against individuals where appropriate.
- 15.4 The Government will not hesitate to bring to the attention of the appropriate authorities any use of its systems by users, which it believes might be illegal.

16 Further Information

- 16.1 If you would like further information on the contents of this Acceptable Use Policy, or on any matters relating to it, please contact the IT Center's Director at 481-5300.

17 History

- 17.1 This Policy was first drafted on the November 7, 2005 and circulated to the Personnel and Legal Departments for comment. The current draft incorporates their comments.
- 17.2 The Policy was first approved by the Government on February 23rd 2006.
- 17.3 There have been no amendments to date.



ENFORCING THE ACCEPTABLE USE POLICY

Enforcing the Acceptable Use Policy
by
Moving to a Domain Network Environment

18 **INTRODUCTION**

- 18.1 To enforce the Acceptable Use Policy, and due to significantly increased security risks, and significant ongoing loss of Government data due to lack of appropriate backing up, the Government IT Center has decided to upgrade the Government Wide Area Network (WAN) to a domain or client-server environment to strictly enforce security to protect the network, and to provide limited automated backup of important Government data.

This is urgently needed and will result in greater security, better management and control of Government's scarce resources, and lower maintenance costs.

19 **BACKGROUND**

- 19.1 The government computer network has become a critical tool in helping in meeting data processing and data communication needs. For this reason, it is important that processes to protect the data, processing and communication facilities be installed and must be distributed throughout the network. For example, sending sensitive files that are protected with stringent access controls on one system, over the network to another system that has no access control protection, defeats the efforts made on the first system. Simply put, the network is only as strong as its weakest link.
- 19.2 Users must ensure that their data and the Local Area Network (LAN) itself are adequately protected. LAN security should be an integral part of the whole LAN, and should be important to all users.
- 19.3 Electronic mail (email), a major application provided by most networks is replacing much of the interoffice, inter-organizational and even international mail that is written on paper and placed in an envelope. This envelope provides some confidentiality between the sender and receiver, and it can even be argued that the integrity of the paper envelope provides the receiver with some degree of assurance that the message was not altered.
- 19.3.1 Using electronic mail does not provide these assurances. Simple transfers on unprotected networks of inadequately protected electronic mail messages can be captured and read or perhaps even altered. For some networks, there can be no assurance that the message actually was sent from the named sender.

- 19.4 Fortunately tools such as encryption, digital signatures, and message authentication codes help solve these problems and can help provide some assurance.

20 PROPOSED SOLUTION

- 20.1 In an effort to secure the government network, the decision has been taken to implement the following Network Security policies. These policies will secure all physical and logical access to government property, including hardware, software, and data.
- 20.1.1 These policies will be strictly enforced by upgrading the current peer-to-peer networks on the WAN to full domain network environment, using domain controllers. These domain controllers will be operating Microsoft Windows 2003 server or similar Network Operating Systems (NOS).

21 Hardware

- 21.1 The responsibility of the physical security of all systems will be given to the Head of each Department. This means access to and movement of computers and any part thereof must be authorized by such person.
- 21.2 Any missing computers and parts must be reported to the Head of Department who will contact the IT Center and also initiate the procedures for investigation and any other procedures used for the theft of government property.
- 21.3 Access will be given to the IT Center, which will take full responsibility for all rooms containing servers and any IT equipment not directly used by users. Any access required by any department will be given on an approved discretionary basis.
- 21.4 Any system not solely serviced and maintained by the IT Center will not be put on the government's network.

22 Software and User Access

- 22.1 All software that do not pertain to the functioning of the Government's operations will be removed from all computers.
- 22.2 All access to removable media will be terminated, except such access is required and authorized by the head of department and the user signs a Non Disclosure Agreement (NDA) (e.g. CDs, DVDs and USB external devices).

- 22.2.1 All access to web based email systems except government's email systems will be terminated e.g. Hotmail.com yahoo mail in a phased manner.
- 22.3 All instant messenger services that do not meet the IT Center security policy will not be installed on the systems.
- 22.4 All users will be furnished with network usernames and passwords, which will be used to secure access to all government data to which they are authorized to have access.
- 22.5 All users will be denied access to the local machine, thereby enforcing automated data backup procedures.

23 BENEFITS

We envision that the following benefits will be derived from this policy;

- 23.1 Centralized management of all computer and network resources
- 23.2 Full data security and integrity
- 23.3 Centralized management of all users
- 23.4 Virus and spyware control
- 23.5 Secure centralized backup of all important government data
- 23.6 Software application protection from conflicting drivers or other software
- 23.7 Operating system protection from conflicting drivers or other software.