

**BY ORDER OF THE COMMANDER**

**AIR FORCE OPERATIONAL TEST AND  
EVALUATION CENTER INSTRUCTION 33-200**

**5 OCTOBER 2004**

**Communications and Information**

**INFORMATION TECHNOLOGY ACCEPTABLE  
USE**



**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: HQ AFOTEC/SCI (Maj Charles Mackin)

Certified by: HQ AFOTEC/SC  
(Lt Col Thomas Floring)

Supersedes AFOTECI 33-200, Oct 02

Pages: 19  
Distribution: F

---

This instruction implements Air Force Policy Directive 33-1, *Command, Control, Communications, and Computer (C4) Systems* and AFD 33-2, *Information Protection*. It provides policy and defines responsibilities for acceptable use of information technology equipment at AFOTEC. This instruction applies to all AFOTEC military and civilian personnel, including contractors, consultants, and temporary workers, making use of government-issued or controlled information technology (IT) equipment or while connected to AFOTEC information systems with personally owned equipment. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force WEB-RIMS Records Disposition Schedule (RDS) located at <http://webrims.amc.af.mil/rds/index.cfm>.

**SUMMARY OF REVISIONS**

**“This publication has been substantially revised and must be completely reviewed”**

**1. General Use and Ownership:**

- 1.1. Prior to being granted access to an AFOTEC network or system, all users must complete an AFOTEC Form 14, AFOTEC Computer Account Access Request, to certify that the appropriate background investigation required by AFI 31-501, Personnel Security Program Management, has been accomplished and mandatory Information Assurance (IA) Awareness training completed. These requirements must be met before granting access to any AFOTEC system, whether standalone or connected to a network.
- 1.2. For security and network maintenance purposes, authorized individuals within AFOTEC may monitor equipment, systems and network traffic.

1.3. Use computer systems for official or authorized purposes only. Supervisors may authorize use of government resources for personal projects if they determine the use is in the best interest of the Air Force, does not interfere with mission performance, and is allowed by the *Uniform Code of Military Justice* (UCMJ) and DoD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4 dated August 6, 1998. This authorization must specify in writing what type of personal processing is authorized, who is authorized to do it, and when it may be done.

1.4. AFOTEC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.5. Only government issued or controlled equipment may be used to connect to an AFOTEC network through a Virtual Private Network (VPN) or the AFOTEC Remote Access Server (RAS). Furthermore, only government issued Personal Digital Assistants (PDA), BlackBerrys, laptops, and other portable electronic devices can be directly connected to an AFOTEC network or network device. The AFOTEC user agreements in [Attachment 2](#), [Attachment 3](#), and [Attachment 4](#) outline further requirements for PDA, BlackBerry, and dial-in remote access use.

1.6. The use of personally owned IT equipment to access an unclassified government e-mail account through Outlook Web Access (WebMail) is authorized with the following restrictions:

1.6.1. The system must employ current antivirus software (available at no cost for military and government employees through the AFOTEC Customer Support Center).

1.6.2. Government-owned sensitive information downloaded or stored on the personally owned equipment must remain on removable media (i.e., a floppy disk, ZIP drive, USB drive, CD-ROM, etc.) and the sensitive information must be marked and protected in accordance with all applicable DoD and Air Force requirements. Examples of sensitive information include Privacy Act, For Official Use Only, Scientific and Technical, Contractor Proprietary, and information about friendly forces' (US, allied, and coalition) activities, intentions, capabilities, and limitations.

1.6.3. Personally owned equipment may not be used to process classified government information.

1.7. Do not permit any unauthorized individual access to a government owned or operated system.

1.8. Access to AFOTEC IT equipment and systems may be denied at the discretion of the AFOTEC Designated Approval Authority (DAA) for personnel who:

1.8.1. Are undergoing disciplinary actions.

1.8.2. Are arrested or involved in a criminal investigation.

1.8.3. Fail to comply with DoD, Air Force, or AFOTEC policies and procedures.

## 2. Security Requirements:

2.1. Authorized users are responsible for the security of their passwords and accounts. Keep passwords secure and do not share accounts. Do not provide your network account password to anyone under any circumstances. AFOTEC Customer Support Center personnel will not ask users to divulge passwords, so be extremely suspicious of anyone requesting your password.

2.2. If a device is password capable, that capability must be activated and configured to meet the following password composition rules:

- 2.2.1. A minimum of eight characters.
  - 2.2.2. At least one capital letter.
  - 2.2.3. At least one lower case letter.
  - 2.2.4. At least one special character (i.e., !, @, #, \$, %, ^, &, \*, etc.).
  - 2.2.5. Must not contain the user name or the user identification (userID).
  - 2.2.6. Must not contain dictionary words spelled frontward, backward, or split with a number or special character.
- 2.3. Passwords must be changed at least quarterly. If your password is compromised or a device you use to access the network is lost or stolen, you must contact the AFOTEC Customer Support Center as soon as possible to have your password changed.
- 2.4. All unattended PCs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less. Users must log off or lock the terminal (control-alt-delete for NT/Win2K/XP users) when the host will be unattended.
- 2.5. All IT equipment used to process government information, whether owned by the individual or government-issued, shall be continually executing approved virus-scanning software with a current virus database unless an approved antivirus product does not exist for the equipment. If there is no approved antivirus product available, then extra care should be taken to virus scan any files or data at the time of their transfer from the device to another system with antivirus capabilities.
- 2.6. Due to the fact that information contained on portable computers is especially vulnerable, special care should be exercised to ensure such computers are kept physically secured at all times. Do not leave portable computers visible in unattended vehicles or rooms. Keep the portable computer with you at all times in public areas and on public transportation. Refer to [Attachment 4](#) for additional guidelines on laptop use.
- 2.7. Do not connect equipment to any AFOTEC network without prior approval of the DAA.
- 2.8. Do not connect any AFOTEC issued or controlled equipment to any non-AFOTEC network without prior approval of the DAA. This includes connecting laptops or other portable electronic devices to Internet Service Provider (ISP) networks (such as America Online, Microsoft Network, etc.) or other government-controlled networks (such as the Kirtland base network) through a dial-in, broadband, or Internet Protocol (IP) connection.
- 2.9. Do not relocate accountable nonportable computer systems without first notifying your equipment custodian (EC).
- 2.10. Do not make any changes to the configuration of any AFOTEC system without prior approval from your information systems security officer (ISSO) or Workgroup Manager (WM). This includes the addition, removal, or disabling of any hardware or software, changes to the cable connections between components, or changes to the default security settings.
- 2.11. Report system security incidents, vulnerabilities, and malicious logic attacks (including viruses, worms, and spyware) to your ISSO, WM, or the AFOTEC Customer Support Center immediately.
- 2.11.1. Security incidents involving classified information that exceeds the approved classification level of the system, otherwise known as Classified Message Incidents (CMI), must also be immediately reported to your unit security manager or AFOTEC/SF. Do not, however, discuss

details of the CMI over an unsecured phone line. If you must make notification over an unsecured phone, identify only your name, location, and the possibility that a CMI has occurred. If the contaminated desktop or laptop system is physically connected to the network through a network cable, you should disconnect that cable to prevent further contamination of the network. Do not turn off the power to the contaminated system as that could purge its memory of essential tracking information. Do not leave the system unattended until your ISSO or WM tells you it is safe to do so.

2.11.2. In the event of a suspected virus, worm or spyware infection, you must immediately stop using the involved computer, physically disconnect the machine from all networks, and contact your ISSO, WM or the Customer Support Center. If the suspected infection appears to be damaging information or software, turn off the computer immediately.

2.12. Clear or destroy media used to store government information according to the procedures outlined in AFSSI 5020, *Remanence Security*, prior to turn-in or disposal of the media (i.e., hard drives, floppy disks, Zip or Jaz disks, CD-ROMs, Universal Serial Bus (USB) storage devices, etc.).

2.13. Do not move or otherwise reposition any of the components of a classified system without prior approval from the ISSO for that system. Doing so could invalidate the emission security countermeasures in place for the system, resulting in a possible security incident.

2.14. Do not use modems in any system physically connected to an AFOTEC network without prior DAA approval. Laptops connecting directly to the network (other than through a dial-in connection) must have the modem card removed or, if the modem is a permanent part of the system, must not be simultaneously connected to the network and a phone line.

2.15. Log off the AFOTEC network at the end of every duty day or whenever you will be away from your network workstation or laptop for more than eight hours.

### 3. E-Mail Use:

3.1. Do not access non-government provided E-mail accounts (i.e., those provided by an ISP, university or college, government contractor, commercial business, etc.) while connected to an AFOTEC network.

3.2. Do not open attachments from unknown senders as an attachment may contain viruses, E-mail bombs, Trojan horses, or other forms of malicious code. Do not save attachments to a network or shared drive prior to virus checking the file.

3.3. If you receive an e-mail containing classified information that exceeds the approved classification level of the system (Classified Message Incident), you must comply with the reporting and safeguarding requirements identified in Paragraph 2.11. of this instruction.

3.4. Limited personal use of government-provided E-mail communication is authorized provided such use meets the following restrictions:

3.4.1. Serves a legitimate Air Force interest.

3.4.2. Does not interfere with the performance of official duties.

3.4.3. Is of reasonable duration and frequency, and, whenever possible, is made during personal time (such as after duty hours or lunch time).

3.4.4. Does not overburden the communications system with large broadcasts or group mailings.

3.4.5. Creates no additional expense to the Air Force or DoD.

3.4.6. Does not reflect adversely on the Air Force or DoD.

3.5. You must receive approval from your supervisor before subscribing to or participating in E-mail list-servers and news groups other than official Air Force internal information products accessible through the Air Force Link web site. Supervisors should ensure the subscription or participation serves a legitimate Air Force interest as it could expose information about AFOTEC's host servers and e-mail domain to potential adversaries on the Internet.

3.6. Official communications (i.e., official memorandums, messages, orders, taskings, letters, etc.) sent via E-mail will follow specific formats found in Air Force Handbook (AFH) 33-337, *The Tongue and Quill*. All official E-mail will include “//SIGNED//” in upper case before the signature block to signify it contains official Air Force information (e.g., instructions, directions, or policies).

3.6.1. Organizational E-mail accounts (i.e., AFOTEC/CC Corporate Account, AFOTEC/SC Corporate Account, etc.) should be used to send official E-mail messages that provide formal direction or establish a formal position, commitment or response for that organization. Senders will include a formal signature block on all E-mail sent from organizational accounts. For example:

//SIGNED//

LARRY D. WILSON, Lt Col, USAF

Chief, Policy Division

Directorate of Policy and Resources

3.6.2. Individual E-mail accounts (i.e., John.Doe@afotec.af.mil) should be used for working communications between individuals that generally do not commit or direct an organization. Individual E-mail typically uses a less formal writing style, but is still considered official when the sender is acting in an authorized capacity. Official communications sent from an individual E-mail account should also include a signature block. For example:

//SIGNED//

LARRY D. WILSON, Lt Col, USAF

Chief, Policy Division

Authorized personal use messages that meet the conditions outlined in Paragraph 3.4. may also be sent from an individual E-mail account, but do not require the use of a signature block.

3.7. Do not use E-mail to send sensitive information across the Internet unless the transmission is encrypted. Examples of sensitive information include Privacy Act, For Official Use Only, Scientific and Technical, Contractor Proprietary, and information about friendly force's (US, allied, and coalition) activities, intentions, capabilities, and limitations. Contact your Workgroup Manager for assistance in using your Common Access Card (CAC) to encrypt sensitive data.

3.8. The following uses of government-provided E-mail are prohibited:

3.8.1. Intentionally or unlawfully misrepresenting your identity or affiliation in E-mail communications.

3.8.2. Distributing copyrighted materials by E-mail or E-mail attachments without consent from the copyright owner. Failure to maintain consent may violate federal copyright infringement laws and could subject the individual to civil liability or criminal prosecution.

3.8.3. Sending or receiving E-mail for commercial or personal financial gain using government systems.

3.8.4. Sending harassing, intimidating, abusive, or offensive material to, or about others.

3.8.5. Causing congestion on the network by such things as the propagation of chain letters, broadcasting inappropriate messages to groups or individuals, or excessive use of the data storage space on the E-mail host server.

3.8.6. Configuring any government issued or controlled system to automatically forward E-mail to a non-government provided E-mail account (such as your personal E-mail account at home).

#### **4. Internet Use**

4.1. Access the Internet only for official business or authorized activities. Anyone making use of an AFOTEC network to access the Internet is subject to monitoring. Unauthorized use can result in disciplinary action.

4.2. All AFOTEC systems with Internet access will be preconfigured with an approved AFOTEC web browser. Do not change any of the default connection settings for this web browser or install any additional web browsing software without prior approval of the DAA.

4.3. Determine the sensitivity of information prior to transmitting it via the Internet and apply the appropriate level of protection required by AFI 33-129, *Transmission of Information Via the Internet*.

4.4. Ensure that all official records created while using the Internet are placed in an official record management system. Contact your record custodian for assistance with identification and proper filing of official records.

4.5. Do not participate in "chat lines" or other open forum discussions on the Internet unless for official purposes and after approval by appropriate Public Affairs channels.

4.6. Users must check all downloaded files for viruses prior to opening them. This applies to sound and video files as well as files attached to E-mail messages. If files are compressed, perform a second check of the files once decompressed. Do not download files to a network or shared drive.

4.7. Do not provide a user ID and password to access a web site unless the transmission is protected through secure sockets layer (SSL) encryption. SSL encryption is normally indicated by an "https://" preceding the web address on the web browser's address line and the presence of a closed padlock icon in the bottom right of the web browser window.

#### **5. Software Use:**

5.1. Do not install and use copies of government-owned software on a personally owned computer unless the software license explicitly allows users to do so and the DAA has authorized such use. When authorized for installation on a home computer, only use the software for official Air Force business. Personal use may be a violation of *The Copyright Act*, rendering the individual user accountable and liable.

5.2. Obtain written approval on an AFOTEC Form 50, **Communications-Computer Systems Requirements Document** prior to installing any software on government systems.

5.3. Do not make any illegal copies of copyrighted software.

**6. 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). The items listed below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

6.1. Under no circumstances are AFOTEC personnel authorized to engage in any activity that is illegal under local, state, federal or international law.

6.2. 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 AFOTEC.

6.3. Storing or processing classified information on any system not approved for classified processing.

6.4. Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes, but is not limited to, racist literature, materials, or symbols, and sexually harassing materials. Obscene material includes, but is not limited to, pornography and other sexually explicit materials.

6.5. Any use of AFOTEC equipment or systems for personal or commercial financial gain. This includes, but is not limited to, chain letters, commercial solicitation, and sales of personal property other than on authorized bulletin boards established for such use.

6.6. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music (i.e., MP3 music files), and the installation of any copyrighted software for which AFOTEC or the end user does not have an active license is strictly prohibited.

6.7. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Consult your supervisor, ISSO or the IA Office prior to exporting any material that is in question.

6.8. Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6.9. Making fraudulent offers of products, items, or services originating from any AFOTEC account.

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

6.11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the individual is not an intended recipient or logging into a server or account that the individual 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.

- 6.12. Using another person's account or identity without appropriate authorization or permission.
- 6.13. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.
- 6.14. Port scanning or security scanning is expressly prohibited unless prior notification to the IA Office is made.
- 6.15. Executing any form of network monitoring which will intercept data not intended for the individual's host, unless this activity is a part of the individual's normal job/duty.
- 6.16. Attempting to circumvent or defeat security or auditing systems and features (such as user authentication) without prior authorization or permission.
- 6.17. Interfering with or denying service to any user other than the individual's host (for example, denial of service attack).
- 6.18. Using any program/script/command or sending messages of any kind with the intent to interfere with or disable a user's terminal session by any means, locally or via the Internet/Intranet/Extranet.
- 6.19. Providing Privacy Act-protected information about AFOTEC personnel to parties outside AFOTEC.
- 6.20. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

**7. Enforcement.** Any individual found to have violated this policy is subject to disciplinary action or termination of employment.

**8. Form Prescribed.** AFOTEC Form 14, AFOTEC Computer Account Access Request.

FELIX DUPRÉ, Major General, USAF  
Commander

**Attachment 1****GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS*****References***

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFPD 33-2, *Information Protection*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-119, *E-Mail Management and Use*

AFI 33-129, *Transmission of Information Via the Internet*

AFI 33-332, *Air Force Privacy Act Program*

AFI 33-202, *The Air Force Computer Security Program*

AFI 33-203, *Emission Security*

AFI 33-204, *Information Assurance (IA) Awareness Program*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFMAN 33-223, *Identification and Authentication*

AFMAN 33-229, *Controlled Access Protection*

AFMAN 37-123, *Management of Records*

AFSSI 5020, *Remanence Security*

AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*

AFSSI 5027, *Network Security Policy*

DoD 5200.1-R, *Information Security Program*

DoD 5400.7-R, *Air Force Supplement, DoD Freedom of Information Act Program*

***Abbreviations and Acronyms***

**AFSSI**—Air Force Systems Security Instruction

**CAC**—Common Access Card

**COMPUSEC**—computer security

**COMSEC**—communications security

**DAA**—designated approval authority

**DoD**—Department of Defense

**EC**—equipment custodian

**EMSEC**—emission security

**FOIA**—Freedom of Information Act

**FOUO**—For Official Use Only

**ISP**—Internet service provider

**ISSO**—information systems security officer

**LAN**—local area network

**PC**—personal computer

**PCMCIA**—Personal Computer Memory Card International Association

**USB**—Universal Serial Bus

**WAN**—wide area network

### *Terms*

**Antiviral Software**—Computer programs designed to prevent, detect, and eradicate computer viruses.

**Audit**—An automatically created journal of information, created by a network's software, which reports events occurring on a system. The data are examined by network and security personnel in order to track system usage, reconstruct sequences of events, identify unauthorized system access attempts, etc.

**Chain Letters**—A fraudulent money-making scheme in which an individual is sent a letter with a list of names in it. The individual is asked to send money to the person at the top of the list, add their name to the bottom of the list, and forward the letter on to a number of other individuals.

**Classified Information**—Any information the unauthorized disclosure of which could cause a significant measure of damage to the security of the United States and its allies. Classified information carries a designation which denotes the level of protection required, i.e., Confidential, Secret, Top Secret, etc.

**Computer Security (COMPUSEC)**—A security discipline the mission of which is to provide standards, guidelines, countermeasure solutions, and training necessary to ensure an acceptable level of protection for electronically processed information and computer system hardware, software, electronic data storage, hard-copy output, connectivity and environment.

**Computer Virus**—A piece of computer code which is designed to make a copy of itself within an existing program and usually perform some type of negative effect on other programs. This effect can be simply a short-term nuisance effect displaying a specific picture or sound, or a devastating attack that can destroy data, fill a disk with random characters, or severely affect components. The term is sometimes used to describe the entire family of programs known as Malicious Logic that includes not only viruses but also such effects as Trojan Horses, Worms, Bombs, etc. (See Malicious Logic.)

**Connectivity**—Electronic or physical connection between two or more computer systems or groups of systems for the purpose of transfer or sharing of data or software capabilities, i.e., LANs, mainframes, minis, modems, etc.

**Designated Approval Authority (DAA)**—The individuals with authority to grant formal approval to operate a computer system. Such approval is required in order to actively operate any computer system used to support DoD functions.

**Desktop (Desktop Computer)**—An individual small computer system, often referred to generically as a

personal computer or PC, including microcomputers and portable systems such as laptop or notebook computers. Some specific examples include IBM PC-emulating systems using MS-DOS, Windows, or OS/2 operating systems as well as Apple-Macintosh and Power PC processors. Desktops are often used, not only as office administrative processors, but also as file and print servers, primary LAN operating system processors units, net routers, etc.

**EMSEC**—The study and control of decipherable electronic signals unintentionally emitted from equipment.

**Hardware**—The architectural components and associated peripheral equipment of a computer system.

**Information System**—Any equipment or interconnected system used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of information. Such systems include computer central processing units (CPU), subordinate processors, peripheral equipment (monitors, printers, etc.), other affiliated hardware, software, system support environments, connectivity, and any other items used in connection with operating, maintaining, or securing electronic data.

**Information Systems Security Officer (ISSO)**—The appointed administrator for the computer security of an information system or group of systems. The scope of the ISSO may be a single large-scale system or network, or any functional area of smaller systems as described by the commander or DAA.

**Local Area Network (LAN)**—A set of interconnected computer systems used in a limited geographical or facility area designed to share data and resources and provide connectivity with other computer systems or LANs.

**Malicious Logic**—Generic name for all types of programs or code that are included or introduced into a system for an unauthorized purpose, i.e., viruses, Trojan Horses, Time Bombs, Worms, etc. Malicious logic may be hidden in such electronic data storage locations as floppy diskettes, electronic bulletin board items, networks, or even vendor-supplied master software.

**Media (Magnetic Media)**—The physical substances used by a computer system upon which data are recorded and read through the use of magnetic fields (i.e., floppy disks, hard disks, magnetic tape, CD-ROM disks, etc.).

**Peripherals**—All equipment connected to or used with a computer system such as monitors, printers, modems, scanners, mouse's, etc.

**Ponzi Scheme**—A fraudulent money-making scheme that involves getting people to invest in something for a guaranteed rate of return and using the money of later investors to pay off the earlier ones.

**Pyramid Scheme**—A fraudulent system of making money that requires an endless stream of recruits for success. Recruits give money to recruiters and enlist fresh recruits to give them money.

**Sensitive information**—Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

**Software**—Instructions, stored on magnetic media, that direct the actions of the computer system.

**Wide Area Network (WAN)**—A network of computer systems, similar to a LAN, but used in a large and

separated geographical area involving multiple networks, bases, cities, or countries.

**Workgroup Manager (WM)**—Appointed individuals who support a functional community (e.g., work centers, flights, squadrons, or organizations) and serve as the first line of help to resolve customers' administrative and technical problems.

**Attachment 2****HQ AFOTEC  
GOVERNMENT-ISSUED PERSONAL DIGITAL ASSISTANT USER'S AGREEMENT**

Date: \_\_\_\_\_

**Applicability:**

This G-PDA agreement applies to all AFOTEC users assigned a G-PDA that is configured to operate within the Headquarters Air Force Operational Test and Evaluation Center network.

**A G-PDA device connected to the AFOTEC network shall be loaded with a standard software configuration. The user agrees to abide by all the terms, actions, and conditions contained in this letter.**

**Background:** Because security features of the G-PDA are limited, specific procedures must be followed to prevent unauthorized use and compromise of the AFOTEC network.

**Specific Agreements:**

1. Ensure the government issued G-PDA is registered with the unit equipment custodian for accountability.
2. If technically possible, maintain a password on the G-PDA according to the system security policy and, when powered on, ensure password protection is activated. Turn off the G-PDA when not in use and physically secure empty G-PDA cradles.
3. Only use a G-PDA to process unclassified information. Safeguard any information used for official business.
4. Do not use G-PDA in classified environments because of their infrared and similar recording capabilities.
5. Only connect the G-PDA to the AFOTEC unclassified network if Air Force or DoD authorized/licensed G-PDA antivirus software is installed with the most current antivirus definition file. Directorate/Detachment Workgroup Managers (WM) or the AFOTEC Help Desk will provide assistance with this.
6. Do not synchronize information on the AF network using a wireless connection.
7. Do not enable any built-in wireless connectivity capability, including infrared, on the G-PDA.
8. Immediately surrender the G-PDA if contaminated with classified information.
9. Report any software abnormalities to the Information Security Systems Officer (ISSO).
10. Do not load software on the G-PDA without prior authorization from the ISSO.

11. Do not collect classified information on G-PDAs.
12. The user agrees to not dual synchronize the G-PDA on both home and government computers.
13. Do not connect to or subscribe to commercial Internet Service Providers for official E-mail services.
14. Consent to monitoring of the G-PDA, (connected to a system that is subject to being monitored).
15. Report any classified message incident on their G-PDA immediately to their ISSO or the AFOTEC Customer Support Center at 846-5642. Any contaminated G-PDA will be confiscated. Since there are currently no approved methods for sanitizing G-PDAs, the device will either be stored until an approved method of sanitizing is available or destroyed.
16. In signing this agreement, the user indicates acceptance of the following conditions:
  - a. The G-PDA is subject to audit at anytime to assure compliance with AF and AFOTEC G-PDA policy.
  - b. All data entered on the G-PDA while performing government business becomes the property of the U.S. Government.
  - c. Failure to meet any of the conditions stated above can result in forfeiture of the G-PDA.

**Notice and Consent Statement:** Do not transmit classified information over unsecured telecommunications systems. Official DoD telecommunications systems are subject to monitoring. Using this telecommunications system or device constitutes consent to monitoring.

**Agreed to By:**

---

User Name/Office Symbol/Phone #

Signature

Date

**Attachment 3**  
**HQ AFOTEC**  
**BLACKBERRY USER'S AGREEMENT**

Date:

**Applicability:**

This BlackBerry User's agreement applies to any handheld BlackBerry, which is configured to download e-mail from the Enterprise BlackBerry Server within the Headquarters Air Force Operational Test and Evaluation Center network.

A BlackBerry Handheld device connected to the AFOTEC network shall be loaded with a standard software configuration. This agreement is applicable to all AFOTEC users that are assigned a BlackBerry.

**Background:**

Because security features of the BlackBerry system are limited, specific user behavior must be followed to prevent unauthorized use of the BlackBerry and compromise of the AFOTEC network.

**Specific Agreements:**

1. The user agrees to follow the written guidance provided to them when they receive a BlackBerry.
2. The user agrees to register the BlackBerry with the unit equipment custodian.
3. The user agrees to not send messages directly between BlackBerry Users using the BlackBerry PIN or to itself except in an emergency or performing duties as a technician.
4. The user agrees to not use the BlackBerry in a classified environment. Furthermore, no classified information or information that involves command and control activities or equipment that is an integral part of a weapon or weapon system is allowed on the BlackBerry under any circumstances.
5. User agrees to not establish an Autoforward on their BlackBerry nor will they install the computer module that enables the computer to practice BlackBerry forwarding.
6. User agrees to not install Desktop Redirector.
7. User agrees to manually switch off the radio transceiver (to prevent creating wireless modem on the BlackBerry before cradling the device by selecting the Aircraft icon "Turn wireless off" and clicking the input wheel. When this has been successfully accomplished, the User will see the

Tower icon “Turn Wireless On.” This process is reversed when the BlackBerry is removed from the cradle for normal, mobile use.

8. The user will not disclose their BlackBerry PIN to others with the exception of AFOTEC/SC or RIM technical support. The BlackBerry PIN is not the same as the paging PIN. The paging PIN is usually issued when the device is issued.

9. The user agrees to keep the BlackBerry password protected as shown below. Be aware that this may limit the symbols used for the BlackBerry password, since they are not all selectable from the BlackBerry standard keyboard. The user password is changed by the following steps:

- a. select Options (Swiss army knife icon, caption at bottom of screen is “ OPTIONS”)  
[select by rolling to it with the thumbwheel then pressing the thumbwheel],
- b. from the list of options select Security,
- c. enter password (minimum 8 alpha-numeric, two of which must be numeric).
- d. select Password field, it will either be Enabled or Disabled. You will be prompted to change options,
- e. select “Enable”,
- f. click thumbwheel to access menu and click “Change Option” ,
- g. select “Enable”,  
type in your password using upper and lower characters, numbers, and symbols. Click thumbwheel to accept.
- h. enter password again,
- i. click thumbwheel,
- j. select Save Options.

10. The user agrees to not change the Security Timeout to be greater than 5 Min.

11. The user agrees to not dual synchronize the BlackBerry on both home and government computers.

12. The user agrees to not add any unauthorized software to the BlackBerry. To add any needed software, user will contact his/her Workgroup Manager (WM).

13. The user agrees to not install any software on the BlackBerry.

14. The user agrees to not install software on the AFOTEC network through the BlackBerry.

15. The user agrees to not deliberately load any file with a .exe, .com, or .bat extension to the BlackBerry.

16. The user agrees to delete any files with an .exe, .com, or .bat extension, which may be accidentally loaded from the BlackBerry to the AFOTEC network. When this happens, there is no need to contact security.

17. The user agrees to place at least their office telephone number in the Owner information and keep it updated.

18. If a BlackBerry is believed to be lost or stolen, the user agrees to change his/her AFOTEC domain password immediately (if the AFOTEC domain password and the BlackBerry password are the same) and report the missing BlackBerry to the AFOTEC Customer Support Center within 24 hours, by calling (505)846-5642. The user agrees to report immediately any potential breaches in security to his/her Information System Security Officer (ISSO).

19. The user agrees to report any software abnormalities to the ISSO.

20. The user agrees to report any classified message incident on their particular BlackBerry immediately to their ISSO or the AFOTEC Customer Support Center at 846-5642. A contaminated BlackBerry must be secured as classified material until approved sanitization procedures can be run on the device to declassify it.

21. The user agrees to provide the BlackBerry to their ISSO, a representative of the AFOTEC/SC, or their WGM immediately upon request.

**Notice and Consent Statement:** Do not transmit classified information over unsecured telecommunications systems. Official DoD telecommunications systems are subject to monitoring. Using this telecommunications system or device constitutes consent to monitoring.

**Agreed to By:**

---

User Name/Office Symbol/Phone #

Signature

Date

**Attachment 4****AFOTEC/SC REMOTE ACCESS RULES**

1. For security and network maintenance purposes, authorized individuals within AFOTEC may monitor equipment, systems and network traffic. Because of the need to protect AFOTEC's network, management cannot guarantee the confidentiality of information stored on any network device belonging to AFOTEC.
2. Only government issued or controlled equipment may be used to connect to an AFOTEC network through a dial-in connection to the Remote Access Server (RAS).
3. Do not permit any unauthorized individual access to a government owned or operated system. Do not leave your computer unattended with a modem turned on and communications software enabled. Do not configure the communications systems to accept in-coming dial-up calls.
4. All PCs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less. Users must log off or lock the terminal (control-alt-delete for NT/Win2K users) when the host will be unattended.
5. Due to the fact that information contained on portable computers is especially vulnerable, special care should be exercised to ensure such computers are kept physically secured at all times. Do not leave portable computers visible in unattended vehicles or rooms. Keep the portable computer with you at all times in public areas and on public transportation.
6. If you receive an e-mail containing classified information that exceeds the approved classification level of the system, you must immediately notify your ISSO or the Customer Support Center at DSN 246-5642. Do not, however, discuss details of the incident over an unsecured phone line. If you must make notification over an unsecured phone, identify only your name, location, and the possibility that a Classified Message Incident (CMI) has occurred. If the contaminated laptop system is connected to the network either physically through a network cable or through a dial-in RAS connection, you should disconnect the cable or terminate the RAS connection to prevent further contamination of the network. Do not turn off the power to the contaminated system as that could purge its memory of essential tracking information. If it is determined that your portable computer has become contaminated with classified information, you will be required to transport the computer to the nearest Air Force facility immediately for safekeeping and/or sanitization.
7. Other than a dial-up RAS connection to the AFOTEC network, do not establish any other interface between a remote computer used for AFOTEC business activities and another network unless prior approval by the Designated Approval Authority (AFOTEC/SC) has been obtained in writing. You are prohibited from accessing Internet service providers or networks from any government-issued computer or

otherwise using these such services to conduct AFOTEC business activities. This prohibition extends to broadband connections offered through lodging facilities, whether on base or commercial. All AFOTEC business Internet electronic mail and Internet surfing must be accomplished through an AFOTEC-managed Internet connection with AFOTEC approved E-mail software.

1. Do not use cellular modems to connect to the AFOTEC network.
2. Do not change the operating system configuration or install new software on a government-issued computer without prior approval of AFOTEC/SC.
3. Computer equipment supplied by AFOTEC must not be altered or added to in any way without prior knowledge and authorization from AFOTEC/SC.
4. Do not download software from dial-up electronic bulletin board systems, the Internet, or other non-AFOTEC systems onto government-issued computers without prior authorization from AFOTEC/SC.
5. Sensitive government information must not be read, discussed, or otherwise exposed in restaurants, on airplanes, on trains, or in other public places where unauthorized people might discover it.
6. All computers used to process government information must be continually executing AFOTEC/SC-approved virus scanning software with a current virus database.
7. If you suspect infection by a virus, or if virus detection software indicates an infection, you must immediately stop using the involved computer, physically disconnect the machine from all networks, and call the Customer Support Center at DSN 246-5642. If the suspected virus appears to be damaging information or software, turn off the computer immediately.
8. Access the Internet only for official business or authorized activities. Anyone making use of an AFOTEC network to access the Internet is subject to monitoring. Unauthorized use can result in disciplinary action.