102nd ISR Group
DGS-MA

General Information Systems Acceptable Use Policy and User Agreement

This agreement is for all users (military, civilian, and contractor) of any and all current and future networks and Information Systems installed and operated at 102 ISRG / DGS-MA. Compliance with this agreement is mandatory.

The **INDIVIDUAL** provides much of the protection for the information contained in the IS. If your security alertness is relaxed at any time, a security violation or compromise may result which could cause grave damage to national security. In the final analysis, system security depends upon **YOU**, the individual user.

Place your initials in left column and digitally sign when completed indicating that you have read and understand this user agreement. Any questions please contact any member of the 102ISRG Information Assurance Office staff.

1. **Purpose.** To emphasize your individual responsibilities when accessing 102ISRG/DGS-MA Site Information Systems (IS) and resources.
2. **General.** The fundamental approach to security of Information Systems is based on the principles of individual accountability and need-to-know. Procedural and technical security features incorporated into systems are required to provide adequate protection for the system and the data contained within.
3. **Policy.** U.S. Government policy requires all classified information be appropriately safeguarded to ensure the confidentiality, integrity, and availability of the information. Safeguards will be applied such that information is accessed only by authorized persons and processes, is used only for authorized purposes, retains its content integrity, is available to satisfy mission requirements, and is appropriately marked and labeled. The combination of security safeguards and procedures shall assure that the system and users are in compliance with ICD, DoD, NSA, DIA, USAF, ANG and 102ISRG Information Systems security guidance and publications.
4. **Individual Responsibilities**. Upon receipt of your userid and password, you will have access to various Information Systems that process and store classified information (For Official Use Only, Confidential, Secret, Top Secret SCI). The burden of responsibility for the security of classified information stored within these system ultimately rests with each person who uses or has access to the system. No matter how elaborate the built-in precautions and safeguards, they provide little security if each person using the system does not enact personal responsibility for security. The following are key requirements and responsibilities of each individual user associated with the 102ISRG/DGS-MA Site:

4.1 General User Requirements:

a. Be a U.S. citizen

4.2 Account Access Control/Information Systems Protection

JT **a. I will not share or permit my logon userid to be used by anyone else.** Individuals requiring temporary or permanent network access should only be provided access through the authorization of the Information Assurance Office.

JT **b. I will accept responsibility for ANY and ALL activity that occurs under my individual User-ID.**

JT **c. I will ONLY use the access or privilege granted to me to perform authorized tasks or mission-related functions.**

JT **d.** User names and passwords will be stored and safe guarded at the same classification level of the Information Systems they permit access.

JT **e.** I will use the system and network, to include access to the Internet, Electronic Mail (E-mail) and network shares for only authorized purposes IAW AFI 33-200, Information Assurance (IA) Management, AFMAN 33-152, User Responsibilities And Guidance For Information Systems, AFI 33-115, Air Force Information Technology (IT) Service Management, and ICD 503.
Reading of the listed documents is highly recommended but not required.

JT **f.** I understand that masking my identity or assuming the identity of another user is strictly prohibited, except by authorized law enforcement personnel.

JT **g.** It is your responsibility to control access and utilization of any "private" files, which you have stored under your User ID/password. **YOU** are accountable for any use made of such files or data and for the correct classification, caveats, and any modifications made to them.

JT **h.** You must not access the accounts of others with the intent to read, browse, modify, copy, or delete files and directories unless they have given you specific authorization to do so. Authorization is a permissions application within the system, not sharing of password(s).

JT **i.** **LOGOFF** properly at the end of each session. If the machine will not give you the required LOGOFF response, inform your ISSO, CMOC or a System Administrator.

JT **j.** You must notify the Information Assurance Office Account Management personnel of TDYs exceeding 30 days or more prior to your departure.

JT **k.** I will not leave my workstation signed on and unattended without at least utilizing the screensaver password screen-locking function. **When leaving at the end of the duty day, I <u>will</u> properly and completely log off the network.**

JT **l.** I will report all security violations, system vulnerabilities, suspicious network activities, and detected viruses to the System Administrator or ISSO.

JT **m.** Report all security incidents to the ISSO, ISSM, SSO or SA

JT **n.** I will comply with all computer and network security guidance issued by my unit and IA Office and will acknowledge this by going to the *IAO office and acknowledging this to the ISSM*.

JT **o.** I will comply with additional policies and procedures prescribed by my ISSO or Unit Security Manager which may be required for operating a classified workstation.

JT **p.** **I Will Immediately Report any and all classified data spillages and computer virus activities to ISSM/ISSO and SSO or ISS CMOC.**

q. All AFDGS and JWICS accounts will expire when your Information Assurance (IA) certificate expires. When re-accomplishing your IA certificate please get the Information Assurance Office a soft copy (saved in landscape format so we can see full date), please e-mail it to the 102ISRG IA Office Niprnet group mailbox: 102 IW/IG Information Assurance Org

JT **4.3 PASSWORDS**

JT **a.** Your password is **<u>FOR YOUR EYES ONLY</u>** and **<u>WILL NOT</u>** be disclosed to, or used by, anyone else regardless of the situation or circumstances.

JT **b.** You **<u>WILL NOT</u>** give out your password nor log on for any individual, whether they have access to the system or not. Such disclosure to, or use by, another is considered a security violation.

JT **c.** **Passwords** will **NOT** be written down or stored in desk drawers, programmed into function keys, part of batch or login scripts, et cetera. A user storing his/her password in this manner will have committed a security violation.

d. Your password must meet the complexity requirement of ICS 500-16 and the Information System you have been granted access to. Generally your password must be a minimum of 14 characters in length, must consist of at least two upper case letters, two lower case letters, two numbers and two special characters (non-alpha/numeric). It cannot contain dictionary words or any information that pertains to you (i.e. date of birth, spouse or child name, pet name, etc.) will not contain multiple repeated characters, full dictionary words (in English or any other languages), names, or well-known dates.

JT **e.** Report any compromise or suspected compromise of a password to the ISSO or ISSM.

JT **f.** **You will change your password at least every 90 days.**

g. **You will protect your password at the classification of the system for which it is assigned.**

JT **4.4 Media Control**

a. All Removable/Magnetic media (floppies, CD-ROM's, etc) will be scanned for viruses using established procedures prior to opening the files on any workstation.

JT **b.** Comply with ALL rules and regulations for scanning all magnetic media that he/she introduces, mails, or transports into or out of the organization.

JT **c.** I will protect all sensitive data (Privacy Act, For Official Use Only or Classified) processed, displayed, printed, or stored at my terminal using the proper guidance.

JT **d.** I will appropriately mark any removable storage media containing sensitive/classified data.

JT **e.** When not in use, I will properly secure FOUO, Privacy Act, sensitive or classified data to prevent inadvertent access.

JT **f.** Provide appropriate classification marking, caveat and safeguard statements on all IS files, output products, and storage media.

JT **g.** All Removable Media for use within a 102ISRG SCIF WILL be issued by the ISSM/ISSO. All media (CD- ROMS, DVDs, Tapes, removed hard drives, OEM install disks, etc.) Entering the SCIF MUST be in-checked with the Information Assurance Office.

JT **h.** Safeguard and report any unexpected or unrecognizable output products to the ISSO, SysAd or ISSM as appropriate. This includes both display and printed products.

JT **i.** Safeguard and report the receipt of any media received through any channel to the appropriate ISSO, SysAd or ISSM for subsequent virus inspection and inclusion into the media control procedures.

JT **j.** All media that is no longer needed or needs to be destroyed will be brought to the Information Assurance Office for destruction. All media leaving the SCIF needs to be out-checked with the Information Assurance Office.

JT **k.** In the event that media that has been issued is lost. That individual that signed out the media MUST report the loss to the ISSM/ISSO, SSO or ISS CMOC as soon as possible.

JT **l.** Suspected misuse or compromise of removable media or information contained therein must be reported to the ISSM/ISSO or SSO immediately.

JT **m.** **Network File Transfers:** All Files needing to be transferred from one network to another (Low to High) may be performed by the user through the DoDIIS One-Way Transfer Service(DOTS). Any other transfers will be performed by the Information Assurance Office.(Contact us for details.) If moving down in classification, if it can't go thru T-MAN then it aint gonna happen! No files will be downgraded from any classified classification to unclassified.

4.5 Email

JT **a.** USAF email systems are provided to support USAF missions. You are only authorized to use email systems for official, authorized government business related to your duties.

JT **b.** You are prohibited from transmitting fraudulent, unethical, harassing, chain letter, or personal messages and files. Do not overburden the e-mail systems with large broadcasts or group mailings.

JT **c.** You must not send any electronic mail or other form of electronic communications by forging another user's identity or attempt to conceal the origin of the message in any way.

JT **d.** Receipt of prohibited or inappropriate electronic mail or files must be reported to the appropriate ISSO.

5. Precautions Following are several specific *precautions* which you must always take in order to protect both yourself and the Information System from possible compromise:

JT **5.1 You MUST practice good OPSEC awareness and consider the OPSEC implications and possible vulnerabilities when posting ANY information to ANY social networking sites or commercial websites.**

JT **5.2** Ensure no other person is in position to see the terminal keyboard while **your password** is being typed.

JT **5.3** Ensure that when you create, file, or store data, regardless of its originator, that the classification and/or special handling caveats correctly apply to all material embedded within the data or file.

JT **5.4** Ensure that any data/file that you store or create does not exceed the overall classification and special handling caveats of the Information System.

JT **5.5** Ensure that all output is handled in accordance with the pertinent document security procedures.

JT **5.6** Before you leave the terminal area, make sure you are logged off, all paper output is removed from the terminal area and properly secured, and any waste is appropriately shredded.

6. Prohibited activities:

JT **6.1 I will not download, install or attempt to configure any software or hardware to either the workstation or network server.**

JT **6.2** **I WILL NOT** attempt to access any files, data, software, devices or network resources which have been readily restricted to me by network permissions and/or software or hardware security mechanisms, or perform a function for which I do not have authorization. **I will not attempt to access, modify or configure any system administration resources installed on any network**.

JT **6.3** **I WILL NOT** leave a live terminal unattended. (Log Off or engage the screen-lock.)

JT **6.4** **I WILL NOT** use your computer system or resource to harass anyone.

JT **6.5** **I WILL NOT** use computer assets for personal or private financial gain or illegal activities, entertainment, or other private pursuits such as gambling, betting, lottery, pornography, or any similar activity.

JT **6.6** **I WILL NOT** play music or video CD/DVDs on government systems.

JT **6.7** **I WILL NOT** Release, Disclose, or Alter information without the consent of the Data Owner or the Disclosure Officer's approval. Violations may result in prosecution of military members under the Uniform Code of Military Justice, Article 92 or appropriate disciplinary action for civilian employees.

JT **6.8** **I WILL NOT** Attempt to strain or test or bypass or circumvent any computer security features or mechanisms. For example, when users leave their workstation unattended without using appropriate screen lock, other users shall not use the system.

JT **6.9** **I WILL NOT** Modify the system equipment or software or use it in any manner other than its intended purpose.

JT **6.10** **I WILL NOT** Relocate or change any IS equipment or the network connectivity of IS equipment without proper security authorization.

JT **6.11** **I WILL NOT** Introduce malicious code into any IS or network.

JT **6.12** **Unauthorized use of software.** You are prohibited from loading any software on any computer system and/or computer network without the approval of the appropriate system administrator. Generally, the system administrator will add new software. This prohibition includes commercial, shareware, freeware, and government-owned software.

JT **6.13** **You are expressly prohibited** from using USAF computers to make illegal copies of licensed or copyrighted software. Copyrighted software must only be used in accordance with its license or purchase agreement. You do not have the right to own or use unauthorized copies of software or make unauthorized copies of software for yourself or others.

JT **6.14** **You are prohibited** from using software that is designed to destroy data, provide unauthorized access to the computer systems, or disrupt computing processes in any other way. The use of viruses, worms, Trojan horses, and other invasive software is expressly forbidden. Systems subject to invasive software are equipped with antivirus software, and users are required to use it. You are prohibited from tampering with or turning off this antivirus software.

JT **6.15 Use of the Information Systems for other than official government business is strictly prohibited and any violation of this prohibition may result in administrative and/or punitive sanctions**.

7. User Training:

JT **7.1** I will ensure that my ***Information Assurance Certification*** stays current.
Failure to do so will result in all your accounts being suspended.

JT **7.2** I will attend/complete additional training as directed: TEMPEST, Annual Information Assurance Briefings, etc.

8. CREW COMM DATA SPILLAGE AND INADVERTENT DISCLOSURE:

JT **8.1** I am aware of the capability of the Crew Comm system to connect to a lower classified level. I will constantly be aware of what security level I am communicating at and will be ever vigilant and mindful of what can and cannot be said.

JT **8.2** In the event of inadvertent disclosure of higher classified data on a lower classified network I will IMMEDIATELY self-report the incident to the Mission Supervisor on duty and the Special Security Officer to initiate the Inadvertent Disclosure process.

JT **8.3** I will not use the "Hot Mic" feature of Crew Comm since Hot Mic is the same as an Open Mic and is a Security Risk.

JT **9. NOTICE AND CONSENT TO MONITORING:** (cao: DTM-08-060, May 9, 2008 /Change 5, 09/25/2013)

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) Information Systems:

- You are accessing a U.S. Government (USG) Information System (IS) (which includes any device attached to this Information System) that is provided for U.S. Government authorized use only.
- You Consent to the following conditions:
  - The U.S. Government routinely intercepts and monitors communications on this Information System for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
  - At any time, the U.S. Government may inspect and seize data stored on this Information System.
  - Communications using, or data stored on, this Information System are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
  - Notwithstanding the above, using an Information System does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
    - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an Information System, regardless of any applicable privilege or confidentiality.
    - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
    - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (Le., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

o All of the above conditions apply regardless of whether the access or use of an Information System includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

I understand that failure to comply with the network security policies and procedures that govern the networks I have access to may result in disciplinary action or loss of network access.

I have completed Information Assurance (IA) Training for the year that I am completing this form. This training must be completed prior to signing this User Agreement. Training will be obtained through the applicable unit.

I have read, understand, and will comply with the terms of this agreement.

Teixeira Jack D	AB E-1
PRINT Last Name, First Name, MI	Rank/Civilian Duty Title

102 ISS	SCOA	508-968-7839
Organization	Office Symbol	Duty Phone

7/15/2021
Date

TEIXEIRA.JACK.DOUGLAS.1539098230
Digitally signed by TEIXEIRA.JACK.DOUGLAS.1539098230
Date: 2021.07.15 15:30:21 -04'00'
Signature of User