USFK JCISA Acceptable Use Policy

1. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in USFK JCISA C2 Systems and Networks from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use.

2. **Access.** Access to USFK JCISA C2 Systems and Networks is for official use and authorized purposes and as set forth in DOD 5500.7-R, "Joint Ethics Regulation", DODD 8500.1, "Information Assurance" or as further limited by this policy.

3. **Revocability.** Access to USFK JCISA C2 Systems and Network resources is a revocable privilege and is subject to content monitoring and security testing.

4. **Applicability.** The USFK JCISA C2 Systems and Network resources provide information processing service for Classified releasable ROK/US. This Acceptable Use Policy applies to ALL ROK and US personnel who are required and are authorized access to the USFK JCISA C2 Systems and network resources.

5. **Classified information processing.** Your assigned government system(s) on USFK JCISA C2 Networks is a classified information system for your organization.

a. Your government system provides classified communication to your organization, the military services, external DOD elements, and other United States Government organizations. Primarily this is done via electronic mail. Your ROKUS classified system is approved to process up to ROKUS classified information only.

b. All government system users are responsible for preventing classified data "spillage." All removable media will be properly marked and these markings checked before use on a classified network. Media that is not marked or is improperly marked will not be used on the network. Data sent in e-mail attachments need to be properly marked, reviewed and verified before being sent over a classified network. Upon review, any question of being releasable will be reviewed and verified by the unit security manager or the foreign disclosure monitor. In the event of a classified data spillage, users will isolate the affected system and contact their security manager immediately.

6. **Personal Identifiable Information (PII) use.** All PII designated by OMB Memorandum 07-16, the Health Insurance portability and Accountability Act of 1996 and the Privacy Act of 1974 will be protected in accordance with DOD 8400.11-R "DOD Privacy Program." PII will not be handled below a For Official Use Only (FOUO) designation.

7. **Minimum security rules, requirements and unacceptable use.** As a government system user, the following minimum security rules and requirements apply. I understand that monitoring of my assigned government system will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.

I understand that the following activities include unacceptable uses of a government information system (IS):

_____ a. Personnel are not permitted access to any government systems unless authorized, trained and only after reading and completing this Acceptable Use Policy. I have completed initial user security awareness training and PII awareness training. I will participate in all training programs as required both before receiving system access and when refresher training is required.

_____ b. I will immediately report the loss/suspected loss, compromised/suspected compromise, or discovery of PII and SI to the first O5 or GS14 in my chain of command and USFK JCISA.

_____ c. I will successfully complete the Personally Identifiable Information (PII) training prior to obtaining access to the USFK JCISA C2 Network(s).

_____ d. I will generate and protect passwords or pass-phrases. Passwords will consist of at least 14 characters with 3 each of uppercase, lowercase, numbers and special characters. I am the only authorized user of my account. I will not share personal accounts and passwords or permit the use of remote access capabilities by any individual.

_____ e. I will use only authorized government hardware and software. I will not install or use any personally owned hardware, software, shareware or public domain software. I will not disable or remove security or protective software or mechanisms and their associated logs. I will not alter, change, configure or use operating systems or programs, except as specifically authorized. I will not introduce executable code (such as, but not limited to .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code. I will not add user-configurable or unauthorized software. I will not attempt to strain, test, circumvent, bypass security mechanisms or perform network traffic monitoring or keystroke monitoring.

_____ f. I will use USFK JCISA provided end point security and virus protection software and procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb drive or any other removable and/or portable storage devices.

_____ g. I will safeguard and mark with appropriate classification level, if required, all information created, copied, stored or disseminated from the information system and will not disseminate it to anyone without a specific need to know. I will not attempt to access or process data exceeding the authorized information system classification level. I will access information only for which I am authorized access to and have the specific need to know. I will not release, disclose or alter information without the consent of the data owner, the original classification authority (OCA) as defined by UNF-CFC Regulation 380-1, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or foreign disclosure officer's approval.

_____ h. I will not utilize DOD provided information systems for commercial use, financial gain or illegal activities. I will not use ISs in any manner that interferes with official duties, undermines readiness, reflects adversely on DOD or violates standards of ethical conduct. I will not intentionally

send, store or propagate sexually explicit, threatening, harassing, political or unofficial public activity communications (LE/CI investigators, attorneys or other official activities operating in their official capacities only, may be exempted from this requirement). I will not participate in other activities inconsistent with public service.

_____ i. I will address any questions regarding policy, responsibilities and duties to my unit IASO. Maintenance of your system will be performed by USFK JCISA personnel and JCISA approved IMOs only. I will use screen locks and log off the system when departing the area.

_____ j. I will immediately report any suspicious output, files, shortcuts or system problems to my unit IASO. I will report all known or suspected security incidents or violations of this Acceptable Use Policy and/or DODD 8500.1 or DODI 8500.2 to the IASO and USFK JCISA.

_____ k. I understand that each information system is the property of the government and is provided to me for official and authorized uses. I further understand that each information system is subject to monitoring for security purposes and to ensure use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the information systems and may have only a limited expectation of privacy in personal data on the information system and may only have a limited expectation of privacy in personal data on the information system. I realize that I should not store data on the information system that I do not want others to see.

8. **Penalties.** I understand that violations of this agreement may be punitive in nature and punishable under Article 92 of the UCMJ or ROK Only UNC/CFC Security Supplement Regulation (as amended 2004.12.01).

9. **Acknowledgement.** I have read the above requirements regarding sue of my assigned government system(s) on the USFK JCISA C2 Network(s). I understand my responsibility regarding my government system(s) and the information contained therein.

_____	_____
Unit/Division/Branch	Date
_____	_____
Last Name, First, MI	Rank/Grade
_____	_____
Signature	Phone Number