USFK Classified CENTRIXS-K (CX-K)
Acceptable Use Policy (AUP)
주한미군사 비밀 CENTRIXS-K (CX-K)
사용인가 약관 (AUP)

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

1. **동의.** 본인은 인가 되지 않거나 부주의한 정보의 사용, 수정, 공개, 파기, 소통 방해 등의 행위들로부터 주한미군사 비밀 CX-K 체계 및 네트워크 내 정보를 보호할 일차적인 의무가 있음을 동의한다.

2. **Access.** Access to USFK Classified CX-K 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.

2. **접근**. 국방성 규정 5500.7-R "합동 윤리 규정", 국방성 훈령 8500.1 "정보보증" 및 본 약관에 따라 주한미군 비밀 CX-K 체계 및 네트워크 접근은 업무 및 인가된 용도에 한 한다.

3. **Revocability**. Access to USFK Classified CX-K Systems and Network resources is a revocable privilege and is subject to content monitoring and security testing.

3. **권한 해제**. 주한미군 비밀 CX-K 체계 및 네트워크는 내용물 감시 및 보안점검이 실시될 수 있으며, 이에 따라 사용자의 접근 권한이 해제될 수 있다.

4. **Applicability.** The USFK Classified CX-K 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 Classified CX-K Systems and network resources.

4. **적용**. 주한미군 비밀 CX-K 체계 및 네트워크는 한미간 기밀 정보처리 담당 체제를 제공한다. 사용인가 약관은 주한미군 비밀 CX-K 체계 및 네트워크에 접근이 필요하고 접근 권한을 허가받은 모든 한미 사용자에게 적용된다.

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

5. **기밀정보처리**. 주한미군 비밀 CX-K 체계는 소속 부서 공무를 위한 비밀정보체계이다.

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.

a. 이 체계는 소속부서, 각 군, 국방부 외부 부서 및 기타 미국 정부 기관에 비밀통신을 제공한다. 이 통신은 일차적으로 이메일로 이루어진다. 한미 비밀체계는 한미 비밀정보 처리용으로 제한한다.

b. All government system users are responsible for preventing classified data "**NDCI**." 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.

b. 체계의 모든 사용자는 비밀 자료 "유출"을 방지할 책임이 있다. 모든 이동저장 매체는 정확히 등급 표기를 해야 하며, 비밀 네트워크에서 사용하기 전에 등급 표기를 확인해야 한다. 등급이 표기되지 않은 매체의 네트워크 상 사용을 금한다. 이메일 및 첨부 파일로 전송할 데이터는 비밀 네트워크로 전송하기 앞서 정확히 등급을 표기, 검토, 검증한다. 데이터 검토 시 해당 부대 보안 담당자 또는 대외 정보공개 담당관이 정보공개 문제를 검토 및 검증한다. 비밀 데이터가 유출될 경우, 사용자는 문제된 체계를 차단하고 즉시 보안 담당자에게 연락한다.

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.

6. **개인식별정보 사용**. OMB 공문 07-16, 1996 년 제정된 건강 보험 양도 및 책임에 관한 법령 및 1974 년 제정된 개인정보 보호법에 따라 모든 개인식별정보는 미 국방부 규정 8400.11-R "미 국방부 개인 정보 보호 강령"에 따라 보호를 받게 된다. 개인식별정보는 보안 등급은 대외비 등급 이상이다.

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.

7. **기본 보안 규칙**. 정부 정보체계 사용자로서 다음과 같은 기본 보안 규칙이 적용된다. 본인은 여러가지 목적을 위해 본인에게 할당된 체계가 감시당할 수 있으며, 감시 중 포착된 정보는 행정, 징계조치 및 형사 기소 목적으로 사용될 수 있음에 동의한다.

I understand that the following activities include unacceptable uses of a government information system (IS): (Initial after each statement.)

본인은 다음의 행위가 정부 정보체계를 사용함에 있어서 용납되지 않음을 숙지한다 (각 항목에 서명).

_____ 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.

_____ a. 사용자 인가, 교육 및 본 사용인가 약관을 숙지, 작성하기 전까지는 체계 접근을 불허한다. 본인은 기초 사용자 보안의식 교육을 수료하였으며, 체계 접근권한을 갖기 전이나 재교육이 필요할 때에 모든 교육 프로그램에 참석하겠다.

_____ 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 Classified.

_____ b. 본인은 주한미군 비밀체계 내 명령체계에 따라 분실 또는 분실이 의심되는 경우, 개인식별정보와 민감한 정보사항의 습득을 O5 (중령급) 또는 GS14 급 군무원에게 즉시 보고한다.

_____ c. I will successfully complete the Personally Identifiable Information (PII) training prior to obtaining access to the USFK Classified CX-K Network(s).

_____ c. 본인은 주한미군 비밀 CX-K 네트워크에 접근 권한을 부여받기에 앞서 개인식별정보 교육을 성공적으로 이수할 것이다.

_____ 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.

_____ d. 본인은 비밀번호를 작성하고 보호하겠다. 비밀번호는 최소 14 자리로 대문자, 소문자, 숫자, 특수문자 각각 3 자리를 포함하여 구성하도록 한다. 본인은 생성된 계정을 단독으로 인가받은 사용자로서 본인의 계정 및 암호를 공유하지 않으며 타인의 사용을 불허하겠다.

_____ 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.

_____ e. 본인은 인가된 하드웨어 및 소프트웨어만을 사용할 것이며, 개인 소유 하드웨어, 소프트웨어, 쉐어웨어 또는 공개 소프트웨어를 절대 설치하거나 사용하지 않겠다. 본인은 보안 또는 보호용 소프트웨어, 매체 또는 관련 로그를 차단하거나 제거하지 않겠다. 특별히 인가되지 않은 이상 운영체계 또는 프로그램을 수정, 변경, 설정, 사용하지 않겠다. 허가 없이 실행가능 코드

(.exe, .com, .vbs, .bat 파일과 같은 유형 및 기타 유형)를 삽입하지 않을 뿐만 아니라 악성코드도 기록하지 않겠따. 본인은 사용자 설정 또는 비인가 소프트웨어를 추가하지 않겠다. 보안장치를 오염, 시험, 회피, 우회하지 않을 것이며, 네트워크 트래픽 감시나 타건 감시를 하지 않겠다.

_____ f. I will use USFK Classified 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.

_____ f. 본인은 모든 체계, 디스켓, 첨부파일, CD, USB 또는 기타 이동 저장장치의 정보를 저장하거나 접근하기 전 주한미군 비밀체계가 제공하는 바이러스 검사 소프트웨어 및 최종 보안 절차를 활용하겠다.

_____ 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.

_____ g. 본인은 생성, 복사, 저장되거나 정보체계에서 파생된 모든 정보를 보호할 것이며 (필요시 올바른 등급 표기) 특별한 사유 없이는 어느 누구에게도 전파하지 않을 것이다. 인가된 정보체계 등급을 초과하는 데이터에 접근하거나 처리하지 않을 것이며, 접근 인가가 있고 필요한 경우에만 정보에 접근하겠다. 본인은 유엔사 및 연합사 규정 380-1 에 의해 정보의 자유 법령 (FOIA)을 집행하는 당국자, 공보실, 대외 공개 담당장교 등과 같은 지휘계통으로 규정된 등급권한부여자(OCA) 즉, 데이터 소유권자의 허가 없이는 정보를 유포, 공개 또는 수정하지 않겠다.

_____ 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.

_____ h. 본인은 미 국방부가 제공한 정보체계를 영리적인 목적 혹은 불법행위의 목적으로 사용하지 않겠다. 공무를 방해하거나, 준비태세를 저하시키거나, 미 국방부에 대한 부정적 영향을 주거나, 윤리 강령 기준을 위배하는 범주의 정보체계 사용을 금하겠다. 본인은 노골적인 성표현, 위협적, 공격적, 정치적, 스팸 메일과 같은 비공식적인 민간업무 통신을 의도적으로 전송, 저장 또는 유포하지 않을

것이며, 이 외에도 공무에 지장을 주는 기타 행위에 개입하지 않겠다. (공무 범주 내에서 체계를 운용하는 LE/CI 관련 조사관, 변호사 또는 기타 공무 책임자는 본 조건에서 제외된다.)

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

_____ i. 본인은 정책, 책무, 의무에 관해서라면 소속 부대 정보보증 담당장교 (IASO)에게 모든 것을 질의하겠다. 체계 정비는 USACISA-P 인원과 USACISA-P 에서 승인한 정보관리담당자 (IMO)에 한하며, 작업 장소를 떠날시 화면 잠금 기능을 사용하고 체계를 로그오프 시키겠다

_____ 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 USACISA-P.

_____ j. 본인은 의심스러운 출력물, 파일, 비정상적인 작업 또는 체계에 이상이 발생할시 즉각 소속 정보보증 담당장교에게 보고하겠다. 본인은 본 인가 사용 약관과 미 국방부 훈령 8500.1 및 미 국방부 지침 8500.2 에 위배되는 행위 및 모든 보안 사고를 정보보증 담당장교 및 USACISA-P 에 보고하겠다.

_____ 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.

_____ k. 본인은 각각의 정보체계가 정부 소유이며, 공무 및 인가된 용도로 사용토록 제공됨을 숙지한다. 또한, 각각의 정보체계는 인가 사용을 보장하고 보안 목적을 위해 감시될 수 있음을 숙지한다. 또한 각각의 정보체계는 인가 사용을 보장하고 보안 목적을 위해 감시될 수 있음을 숙지한다. 본인은 정보체계 내 공무 데이터에 관련하여 프라이버시가 인정될 수 없으며 정보체계 내 개인 데이터 범주에 한해서 제한적으로 프라이버시를 보장받을 수 있음을 숙지한다. 본인은 타인에게 노출되기 싫은 데이터를 정보체계에 저장할 수 없음을 숙지한다.

Webcam Use Policy:

웹캠 사용 약관:

_____ a. Only use the webcam equipment for official business.

_____ a. 웹캠 장비는 공무를 위해서만 사용한다.

_____ b. Ensure all individuals within the work area are notified.

_____ b. 같은 작업 공간에 있는 모든 인원에게 웹캠 사용을 공지한다.

_____ c. Display a sign to ensure all personnel entering the work area are aware that a webcam is in use.

_____ c. 해당 작업 공간을 출입하는 인원이 웹캠 사용을 인지할 수 있도록 표지한다.

_____ d. Remove from the camera field of view or fully cover sensitive and classified information that is not part of the collaborative session, accounting for cameras with hardware or software-based pan and zoom capabilities. This includes moving, fully covering or powering off displays that either show such information or have a classification marking that may give the impression that information inappropriate to the collaborative session may be shown.

_____ d. 회의 내용과 관련되지 않은 비밀 정보는 카메라 화면에서 확대 기능까지 고려해서 치우거나 보이지 않게 한다. 비밀 정보나 회의에 알맞지 않은 등급의 정보는 이동 및 엄호시키거나 정보를 전시하는 화면을 정지한다.

_____ e. Ensure user's side of the session is protected from inadvertent transmission disclosure. Users will close office doors and blinds to minimize this risk.

_____ e. 사용자 쪽에서 정보 유출이 발생하지 않도록 한다. 사용자는 사무실 문을 닫고 블라인드를 내려서 위험을 최소화한다.

_____ f. Verify all attendees of the session have a need to know for all information passed during the session.

_____ f. 회의의 모든 참여자들은 다루는 정보에 대한 인가가 필요하다.

_____ g. Ensure no unrelated conversations can be picked up by the microphone.

_____ g. 관련없는 대화가 마이크를 통하지 않도록 한다.

_____ h. Mute or disconnect microphones/headsets from systems and cover or disconnect webcams when not in use.

_____ h. 사용하지 않을 때는 마이크/헤드셋 및 웹캠을 컴퓨터에서 분리한다.

_____ i. Move, fully cover or power off displays that have a classification marking that could give the impression of a differing classification level than that of the webcam session.

_____ i. 웹캠 회의와 다른 등급을 암시하는 모든 표시를 이동, 엄호 및 정지하도록 한다.

_____ j. Remain cognizant of the session's classification level.

_____ j. 회의의 비밀 등급을 항상 인지한다.

_____ k. Mute microphones when not speaking.

_____ k. 말하지 않을 때는 마이크에 소리를 차단한다.

_____ l. Avoid leaving an active webcam session unattended.

_____ l. 웹캠 회의 진행 중에는 자리를 비우지 않도록 한다.

_____ m. Avoid recording the webcam session, unless the recording meets a specific and official purpose. Ensure recorded files are properly handled and marked IAW classification level.

_____ m. 공무 외에는 웹캠 회의를 녹화하지 않도록 한다. 비밀 등급에 의거 파일을 표시 및 관리한다.

_____ n. Avoid using unclassified audio, video, telephone, mobile or cellular device in the vicinity of a classified webcam session.

_____ n. 평문 음성, 영상, 전화 및 핸드폰을 비밀 웹캠 회의 근처에서 사용하지 않도록 한다.

_____ o. Power off, de-activate or disable all webcam system devices.

_____ o. 모든 웹캠 장비는 정지시키도록 한다.

_____ p. Cover the camera lens and/or point cameras to a wall, corner or ceiling where room activities and sensitive or classified information are not visible.

_____ p. 카메라 렌즈를 덮거나 카메라를 업무 및 비밀 정보가 보이지 않도록 벽이나 천장을 향하게 한다.

_____ q. Report any unauthorized or improper use of webcam equipment to the unit ISSM, Security Manager, or J632 Cybersecurity.

_____ q. 웹캠 장비를 허가되지 않거나 잘못된 방법으로 사용하는 일은 부대 ISSM, 보안 담당자, 또는 J632 사이버보안과로 보고한다.

_____ r. Failure to use webcam equipment securely may result in immediate termination of connectivity and disciplinary action, IAW applicable laws and regulations.

_____ r. 웹캠 장비 관련 보안을 위반하면 해당 규정에 의거 즉시 권한이 차단되며 징계가 따른다.

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).

8. **처벌**. 본인은 본 협약 위반시 미군복무규율 92 조 혹은 2004 년 12 월에 개정된 한국군용 유엔사/연합사 보안업무시행규칙에 의거 실제적인 형벌이나 처벌이 가해질 수 있음을 숙지한다.

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

9. 인정. 본인은 본인에게 할당된 주한미군 비밀 지휘통제 네트워크에서 인가된 정보체계를 사용하는 것과 관련된 상기의 필수조항을 숙지하였으며, 정부가 운영하는 정보체계 및 그 안에 포함된 정보에 관한 본인의 책임을 숙지한다.

_____	_____
Unit/Division/Branch 부대/처/과	Date 일자
_____	_____
Last Name, First, MI 성, 이름	Rank/Grade 계급
_____	_____
Signature 서명	Phone Number 연락처