MIRA SPACE

정보처리 및 정보보호 규정

위성·지상국·소스코드·고객·개인정보 통합보호 기준

문서번호	MIRA-SEC-001
주관부서	전략기획·경영지원·안전보건 담당
제정일	2026. 6. 13.
시행일	2026. 6. 13.
승인	대표이사 최요셉 (서명/인)

주식회사 미라스페이스 (MIRA SPACE Inc.)
서울특별시 강남구 언주로104길 21, 3층
support@miraspace.ai | 02-569-2501

Public Release

제정·개정 이력

구분	일자	주요 내용	작성/검토/승인
제정	2026. 6. 13.	최초 제정	작성: 박현우 / 검토: 김재형 / 승인: 최요셉
개정	-	-	-

제1장 총칙

제1조(목적) 회사의 정보자산, 개인정보, 영업비밀, 위성·지상국 임무정보 및 소스코드를 안전하게 처리하여 유출·변조·오용·서비스 중단을 예방한다.

제2조(적용범위) 임직원, 협력사, 인턴, 교육운영자 및 회사 정보에 접근하는 모든 사람과 회사가 소유·임차·사용하는 기기, 시스템, 클라우드, 저장매체, 문서에 적용한다.

제3조(기본원칙) 목적 명확성, 최소수집, 최소권한, 직무분리, 암호화, 추적가능성, 정확성, 보유기간 제한, 안전한 폐기 및 사고 신속 대응을 원칙으로 한다.

제4조(정보등급) 정보를 공개, 내부, 기밀, 임무중요로 분류한다. 설계도면, 소스코드, 암호키, 위성 명령, 지상국 자격증명, 미공개 시험결과, 수출통제 가능 기술자료 및 민감 개인정보는 기밀 또는 임무중요로 관리한다.

제2장 책임과 접근권한

제5조(대표이사와 정보보호 책임자) 대표이사는 정책과 자원을 승인하며, 정보보호 책임자는 위험관리, 권한, 교육, 점검 및 사고대응을 총괄한다.

제6조(정보자산 책임자) 각 시스템·데이터·프로젝트의 책임자는 정보등급, 허용사용자, 보존기간, 백업 및 외부공유 조건을 정한다.

제7조(사용자 책임) 사용자는 계정·기기를 타인과 공유하지 않고, 의심스러운 메일·접속·분실·오발송·변조·악성코드 또는 무단접근을 즉시 보고한다.

제8조(권한관리) 입사·이동·퇴사와 프로젝트 변경 시 승인된 최소권한만 부여·변경·회수한다. 관리자권한과 임무중요 시스템은 정기 검토하고 다중인증을 우선 적용한다.

제3장 정보 처리와 저장

제9조(수집과 이용) 개인정보와 업무정보는 적법하고 명확한 목적에 필요한 최소한으로 수집·이용하며 목적 외 이용은 승인과 적법 근거 없이 금지한다.

제10조(저장과 전송) 기밀·임무중요 정보는 회사가 승인한 저장소와 암호화된 통신수단을 사용한다. 개인 이메일, 미승인 메신저, 공개 링크 또는 임의 클라우드에 저장·전송하지 않는다.

제11조(문서와 출력물) 기밀 문서는 등급·소유부서·배포범위를 표시하고 출력·복사·반출을 제한한다. 폐기 시 파쇄 또는 복구불가능한 방법을 사용한다.

제12조(이동식 매체와 개인기기) USB·외장저장장치와 개인기기는 원칙적으로 제한하며, 업무상 필요한 경우 승인·암호화·악성코드 점검·반출입기록을 적용한다.

제13조(클라우드·SaaS·협업도구) 보안·개인정보·데이터 위치·백업·삭제·계약종료 시 반환과 파기 조건을 검토한 승인 서비스만 사용한다.

제4장 우주기술·임무정보 보호

제14조(소스코드와 형상관리) 소스코드는 승인된 저장소에서 계정별로 관리하고, 코드리뷰·브랜치 보호·비밀정보 탐지·백업을 적용한다. 암호키와 비밀번호를 코드에 직접 저장하지 않는다.

제15조(위성 명령과 인증정보) 텔레커맨드, 암호키, 호출부호, 주파수 설정, 인증토큰 및 지상국 접속정보는 임무중요 정보로 관리하고 생성·배포·교체·폐기 기록을 유지한다.

제16조(텔레메트리·영상·운용로그) 원본성, 시간동기, 접근권한, 무결성 및 보존정책을 관리하고, 시험·비행 데이터의 삭제·변조·선별 은폐를 금지한다.

제17조(지상국과 운용환경) 운용용 네트워크와 일반업무망을 가능한 범위에서 분리하고, 원격접속은 승인·다중인증·로그기록을 적용한다. 임무중요 작업은 역할분리와 2인 확인을 적용할 수 있다.

제18조(기술이전과 수출통제) 해외 인원·기관·클라우드·회의·교육에 기술자료를 제공하기 전 계약, 비밀유지, 최종사용자, 수출통제 및 국가핵심·전략기술 해당 가능성을 검토한다.

제5장 개인정보·AI·제3자

제19조(개인정보 보호) 임직원, 지원자, 고객, 교육생·보호자 및 방문자의 개인정보는 수집목적, 항목, 보유기간, 제공·위탁 및 권리행사 절차를 명확히 하고 안전하게 보호한다.

제20조(교육생과 촬영정보) 미성년자 정보, 사진·영상, 위치, 성적·평가자료는 보호자 동의와 프로그램 운영에 필요한 범위에서 처리하고 홍보 목적 이용은 별도로 구분한다.

제21조(AI 도구 사용) 외부 생성형 AI나 분석서비스에 기밀, 개인정보, 소스코드, 미공개 임무자료를 입력하지 않는다. 승인된 사용에서도 결과의 오류·편향·지식재산권·보안위험을 사람이 검토한다.

제22조(외부업체와 공동연구) 제3자에게 정보처리를 위탁하거나 공동사용하는 경우 목적, 범위, 보안수준, 재위탁, 사고통지, 감사권, 반환·파기 및 책임을 계약에 반영한다.

제6장 보안운영과 사고대응

제23조(기기·계정 보안) 업데이트, 화면잠금, 악성코드 방지, 디스크 암호화, 강한 인증, 로그와 백업 등 위험에 비례한 보호조치를 적용한다.

제24조(백업과 복구) 핵심 소스코드, 설계·시험·계약·회계·임무데이터는 정기 백업하고 복구 가능성을 점검한다. 백업은 운영환경과 분리하거나 별도 권한으로 보호한다.

제25조(사고보고) 분실, 오발송, 피싱, 계정탈취, 랜섬웨어, 개인정보 유출, 명령·텔레메트리 이상 또는 무단접근 의심 시 즉시 정보보호 책임자에게 보고하고 임의로 은폐·삭제하지 않는다.

제26조(대응절차) 사고 식별 → 확산차단 → 증거보존 → 영향평가 → 복구 → 관계자·기관 통지 → 원인분석 → 재발방지 순으로 대응한다.

제27조(보존과 폐기) 법령, 계약, 분쟁, 연구개발 및 임무 요구를 고려하여 보존기간을 정하고, 기간 종료 후 승인된 방법으로 파기한다.

제28조(교육과 점검) 신규입사자와 전 임직원에게 정기교육을 실시하고, 피싱훈련, 권한점검, 취약점·백업·로그·외부공유 점검을 수행할 수 있다.

제29조(위반과 예외) 위반 시 접근차단, 회수, 조사, 재교육, 계약 또는 인사상 조치를 할 수 있다. 업무상 예외는 위험과 보완조치를 문서화하여 정보보호 책임자의 승인을 받아야 한다.

제30조(시행과 개정) 본 규정은 대표이사의 승인일부터 시행하며, 법령·기술·위협·사업변경 또는 사고 발생 시 검토·개정한다.

별표 1. 정보등급 및 처리기준

기본

등급	예시	저장·전송	외부공유	폐기
공개	승인된 보도자료, 홈페이지 콘텐츠	일반 시스템	승인 후 가능	일반 폐기
내부	일반 업무자료, 회의자료	회사 승인 시스템	업무 필요·승인	삭제/파쇄
기밀	설계, 계약, 소스코드, 고객·개인정보	접근통제·암호화	NDA·책임자 승인	복구불가 삭제/파쇄
임무중요	위성 명령, 암호키, 지상국 자격증명, 미공개 비행데이터	강화된 권한·암호화·로그	원칙 금지, 특별승인	2인 확인·폐기기록

출력물 및 서류 등 보안 관련 NDA 내용 참조

1. Public Release / 공개 배포용

© 2025. Mira Space Inc. All rights reserved.
Disclosure to third parties of this document or any part thereof, or the use of any information contained herein for purposes other than those explicitly authorized by Mira Space Inc. is strictly prohibited without prior written consent.
Public Release

© 2025. Mira Space Inc. All rights reserved.
본 문서 또는 그 일부를 제3자에게 공개하거나, Mira Space Inc.에서 명시적으로 허가한 목적 외의 용도로 사용하는 것은 사전 서면 동의 없이는 엄격히 금지됩니다.
공개 배포용

2. Internal Use Only / 내부 배포용

© 2025. Mira Space Inc. All rights reserved.
This document is intended for internal use within Mira Space Inc. only. Unauthorized disclosure, duplication, or distribution outside the organization is strictly prohibited.
Internal Use Only

© 2025. Mira Space Inc. All rights reserved.
본 문서는 Mira Space Inc. 내부 사용을 목적으로 합니다. 조직 외부로의 무단 공개, 복제 또는 배포는 엄격히 금지됩니다.
내부 배포용

3. Confidential Level 1 / 기밀 등급 1

© 2025. Mira Space Inc. All rights reserved.
This document contains confidential information of Mira Space Inc. and is classified as Confidential Level 1. Unauthorized access, use, or disclosure is strictly prohibited and may result in legal consequences.
Confidential – Level 1

© 2025. Mira Space Inc. All rights reserved.
본 문서는 Mira Space Inc.의 기밀 정보를 포함하며, 기밀 등급 1로 분류됩니다. 무단 접근, 사용 또는 공개는 엄격히 금지되며 법적 책임이 따를 수 있습니다.
기밀 - 등급 1

4. Confidential Level 2 / 기밀 등급 2

© 2025. Mira Space Inc. All rights reserved.
This document contains sensitive business and technical information of Mira Space Inc. and is classified as Confidential Level 2. Distribution is restricted to authorized personnel only.
Confidential – Level 2

© 2025. Mira Space Inc. All rights reserved.
본 문서는 Mira Space Inc.의 민감한 사업 및 기술 정보를 포함하며, 기밀 등급 2로 분류됩니다.
지정된 승인 인원에게만 배포가 허용됩니다.
기밀 - 등급 2

5. Confidential Level 3 / 기밀 등급 3

© 2025. Mira Space Inc. All rights reserved.
This document contains highly sensitive and proprietary information of Mira Space Inc. and is classified as Confidential Level 3. Access is strictly limited and monitored.
Any unauthorized handling will be subject to investigation.
Confidential – Level 3

© 2025. Mira Space Inc. All rights reserved.
본 문서는 Mira Space Inc.의 고도의 민감하고 독점적인 정보를 포함하며, 기밀 3등급(Confidential Level 3) 으로 분류됩니다.
접근은 엄격히 제한·모니터링됩니다.
무단 취급 시 조사 대상이 됩니다.
기밀 - 3등급

별지 1. 정보보안 사고 초기보고서

항목	내용
발견일시·보고자	
사고유형	☐ 분실 ☐ 오발송 ☐ 계정탈취 ☐ 악성코드 ☐ 개인정보 ☐ 임무시스템 ☐ 기타
영향 시스템·정보	
현재 상태와 즉시조치	
외부 노출·대상자	
보존한 로그·증거	
추가 지원·의사결정	