Cloudturing

클라우드 보안 백서

현재 운영 통제와 공동책임

문서 목적

본 백서는 Cloudturing SaaS의 현재 보안 아키텍처, 데이터 보호, 인증·권한, 감사·모니터링 및 AI 안전 통제를 고객과 이해관계자가 일관되게 이해할 수 있도록 설명합니다.

문서 버전	2.1
기준일	2026년 7월 31일
공개 등급	고객 및 일반 공개
운영 주체	꿈많은청년들
문의	cto@cloudturing.com

중요 고지

- 본 문서는 기준일 현재 확인된 Cloudturing의 기술적·운영적 통제를 설명하는 정보 제공 문서이며, 계약상 보증·감사보고서·법률 의견 또는 인증서를 대체하지 않습니다.
- Cloudturing은 클라우드서비스 보안인증(CSAP) 취득을 준비하고 있습니다. 본 문서나 준비 활동은 CSAP 취득, 등급, 인증범위 또는 취득 시점을 보증하지 않습니다.
- Google Cloud Platform(GCP)이 보유한 인증과 Cloudturing SaaS 자체의 인증은 구분됩니다. CSAP 표시는 공식 인증절차를 거쳐 인증받은 서비스에 한하여 사용할 수 있습니다 (KISA CSAP 제도소개 참조).
- 보안상 공개가 적절하지 않은 비공개 도메인, 내부 식별자, 세부 토폴로지와 탐지 기준은 통제 목적과 보호 방식 중심으로 범주화했습니다.
- 고객별 데이터 처리, 보존, 가용성, 사고 통지와 감사자료 제공의 구체적인 의무는 적용 법령과 체결된 계약·약관·개인정보처리방침을 따릅니다.

Contents

1 문서 범위와 보안 원칙

1.1 서비스 개요

Cloudturing은 웹사이트와 디지털 채널에 AI 챗봇을 생성·구성·배포할 수 있는 노코드·로우코드 SaaS입니다. 고객 관리자는 웹 콘솔에서 챗봇, 인텐트, 콘텐츠, 외부 연동과 접근정책을 관리하고, 최종 이용자는 웹 위젯 또는 연동 채널을 통해 챗봇과 상호작용합니다.

본 백서의 기술 범위는 다음을 포함합니다.

- Cloudturing 운영 웹 서비스와 관리 콘솔
- 사용자 인증, 서버 세션과 챗봇 멤버십
- 관리형 클라우드 기반의 네트워크, 실행환경, 데이터 저장소와 로그
- 고객 콘텐츠 업로드·다운로드와 외부 API 연동
- 외부 AI 서비스를 이용하는 AI 처리와 RAG 검색 경로
- 고객별 감사기록, 운영 모니터링, 백업과 복구 기반

1.2 보안 설계 원칙

원칙	Cloudturing에서의 적용 방식
신원 기반 접근	네트워크 위치만 신뢰하지 않고 사용자 세션, 계정 상태, 챗봇 멤버십과 역할을 서버에서 확인합니다.
최소 데이터 처리	서비스 제공에 필요한 범위에서 데이터를 처리하고, 설정에 따라 개인정보 마스킹과 대화 비저장 기능을 제공합니다.
논리적 테넌트 격리	고객·챗봇 범위를 서버 권한검사와 각 데이터 처리 계층에 일관되게 적용합니다.
심층 방어	TLS, 관리형 외부 경계, 비공개 실행환경, 애플리케이션 권한검사와 감사로그를 서로 다른 방어 계층으로 사용합니다.
추적 가능성	인증·관리·사용량·AI 호출과 주요 설정 변경을 운영로그와 고객 감사기록으로 연결합니다.
공동책임	GCP, Cloudturing과 고객이 각각 통제할 수 있는 계정·데이터·애플리케이션·이용환경의 책임을 구분합니다.

1.3 공동책임 모델

주체	주요 책임	예시
기반 클라우드	물리 데이터센터, 하드웨어, 하이퍼바이저와 관리형 서비스 기반 보호	기본 저장 암호화, 네트워크와 관리형 실행·저장 서비스
Cloudturing	SaaS 애플리케이션, 사용자 인증, 권한, 데이터 흐름, 로그, 백업 설정과 공급자 연동	세션 검증, 멤버십 확인, 업로드 승인, 테넌트 범위, 고객 감사기록
고객	사용자·멤버 관리, 업로드 데이터의 적법성, 챗봇 설정, 외부 API와 최종 이용환경	퇴사자 회수, 관리자 권한 관리, 네트워크 접근정책, 외부 API 자격증명

2 현재 보안 아키텍처

2.1 주요 구성

보안 계층	현재 역할과 통제
외부 서비스 경계	관리형 TLS, 요청 라우팅, 상태 확인과 접근 로그
애플리케이션 실행환경	외부에서 직접 접근할 수 없는 실행 계층, 워크로드 신원, 상태 점검과 자원 제한
업로드 처리 경계	파일 승인·검사·변환을 일반 애플리케이션 처리와 분리
업무 데이터 계층	계정과 챗봇 설정 저장, 암호화 연결, 접근통제와 정기 백업
로그·분석 계층	인증, 사용량, AI 호출, 감사와 운영 이벤트의 목적별 기록
객체·캐시·검색 계층	고객 파일, 단기 세션·대화 문맥과 테넌트 범위 검색 데이터 처리
AI 공급자 경계	승인된 애플리케이션 경로에서 AI 추론과 구조화 응답 처리

2.2 요청과 데이터 흐름

대표 요청 흐름

사용자 브라우저 → 관리형 TLS 경계 → Cloudturing 애플리케이션 → 권한·범위 검증 → 데이터 계층·AI 공급자

1. 외부 요청은 관리형 인증서가 연결된 서비스 경계에서 TLS로 보호됩니다.

2. 애플리케이션은 서버 세션, 사용자, 챗봇 멤버십과 요청 범위를 확인합니다.
3. 업무 데이터는 목적과 수명주기에 따라 분리된 저장·검색·로그 계층에서 처리됩니다.
4. AI 기능은 필요한 문맥만 공급자에게 전달하고, 응답 구조와 실행 가능한 동작을 애플리케이션 코드에서 다시 검증합니다.

2.3 환경 구분

운영 환경과 비운영 환경은 배포 대상, 데이터 영역과 주요 저장 경로를 논리적으로 구분합니다. 비운영 환경의 도메인과 내부 식별자는 공개하지 않습니다.

환경 격리의 해석

운영과 비운영 환경은 논리적으로 구분되지만 일부 관리형 기반을 공유할 수 있습니다. 따라서 본 백서는 두 환경이 물리적으로 완전히 분리됐다고 주장하지 않습니다. 운영 데이터 접근은 애플리케이션 권한과 클라우드 신원정책으로 통제합니다.

3 신원, 인증과 접근 제어

3.1 고객 사용자 인증

Cloudturing은 고객 계정 비밀번호를 직접 저장하는 전통적인 비밀번호 로그인을 기본으로 사용하지 않습니다.

- **Google 로그인**: 공급자 토큰의 서명과 대상 서비스를 서버에서 검증합니다.
- **이메일 로그인**: 암호학적으로 생성된 일회용 코드는 짧은 유효기간과 재사용 방지 정책을 적용합니다.
- **서버 세션**: 인증 성공 시 예측하기 어려운 새 세션을 발급하고, 보호된 쿠키와 서버 측 만료·사용자 상태 검사를 적용합니다.
- **세션 회수**: 운영 관리자는 특정 사용자의 활성 세션을 확인하고 회수할 수 있습니다.

3.2 관리자 신원

사내 Google Workspace 계정에는 MFA 정책을 적용합니다. 관리자 애플리케이션은 서버 세션의 만료와 조직 도메인을 확인하고, 주요 변경 요청에서 동일 출처와 요청 콘텐츠 유형을 검증합니다.

3.3 챗봇 멤버십과 역할

고객 영역은 소유자, 일반 멤버와 초대 상태를 구분합니다. 관리자 전용 작업과 일반 멤버 작업을 구분하며, 콘텐츠 관리·다운로드·보안설정과 결제 관련 주요 경로는 서버에서 챗봇 멤버십과 역할을 확인합니다.

고객 소유자는 자기 챗봇의 멤버 목록을 확인하고 초대·거절·제거할 수 있습니다. 클라이언트가 전달한 식별자만을 권한 근거로 사용하지 않고, 서버 세션과 저장된 멤버십을 결합해 판단합니다.

3.4 클라우드 워크로드 신원

클라우드 워크로드는 장기 서비스계정 키 파일 대신 연합 신원과 단기 자격증명을 사용합니다. 기준일 점검에서 운영에 사용하는 클라우드 서비스계정에 사용자 관리형 장기 키가 존재하지 않았습니다.

4 네트워크와 플랫폼 보안

4.1 외부 경계

- 외부 웹 트래픽은 관리형 서비스 경계를 통해 애플리케이션으로 전달됩니다.
- 운영 도메인에는 관리형 TLS 인증서의 발급·갱신 체계를 사용합니다.
- 웹 응답에는 HSTS를 적용하고 불필요한 서버 식별정보를 줄입니다.
- 주요 외부 경계는 요청 로그와 상태 확인을 사용합니다.

4.2 실행환경 경계

- 주요 애플리케이션 실행 노드는 외부에서 직접 접근할 수 없는 사설 경계에 둡니다.
- 플랫폼 무결성 보호와 관리형 업데이트 채널을 사용합니다.
- 개별 내부 서비스는 외부에 직접 노출하지 않고 서비스 경계를 통해서만 연결합니다.
- 워크로드에는 자원 요청·한도, 시작·생존·준비 상태 확인과 시스템 모니터링을 적용합니다.

4.3 관리 접근과 고객 접근정책

고객은 챗봇별로 허용 도메인과 IP/CIDR 접근규칙을 설정할 수 있습니다. 도메인 규칙은 정확한 호스트, 하위 도메인 포함과 제한된 와일드카드 방식을 지원합니다. 보안설정 변경은 관리자 권한을 요구하며, 네트워크 차단과 주요 보안설정 변경은 감사기록과 운영 통지에 연결됩니다.

네트워크 통제의 범위

네트워크 통제는 서비스 노출도, 경로와 위험도에 따라 다르게 적용합니다. 본 백서는 모든 경로에 동일한 통제 또는 전용 보안제품이 적용된다고 주장하지 않습니다. 외부 경계는 관리형 TLS, 사설 실행환경, 내부 서비스와 애플리케이션 신원·권한검사를 조합해 보호합니다.

5 데이터 보호와 개인정보

5.1 전송 중 암호화

구간	현재 보호 방식
브라우저 ↔ 서비스 경계	HTTPS와 관리형 TLS 인증서
서비스 경계 ↔ 실행환경	클라우드 내부의 관리형 백엔드 연결
애플리케이션 ↔ 업무 데이터	암호화 연결과 신원 기반 데이터베이스 인증
애플리케이션 ↔ 클라우드 API	공식 클라이언트 또는 HTTPS API와 단기 자격증명
Cloudturing ↔ 외부 API	HTTPS와 연동별로 합의된 인증방식

5.2 저장 데이터 암호화

주요 업무 데이터, 로그, 객체와 플랫폼 저장 계층은 Google Cloud의 기본 저장 암호화를 상속합니다. Google Cloud는 고객 콘텐츠를 별도 고객 조작 없이 저장 계층에서 암호화한다고 설명합니다.[1]

현재 문서에서 "암호화됨"은 Google 소유·관리 키를 사용하는 기본 저장 암호화를 포함하며, 모든 저장소에 고객 관리형 암호화 키(CMEK)가 적용됐다는 의미는 아닙니다.

5.3 데이터 위치와 외부 처리

Cloudturing의 주요 트랜잭션 데이터, 애플리케이션 로그와 고객 파일 저장소는 대한민국 서울 리전을 중심으로 구성합니다. 다만 다음 처리에는 별도 공급자 또는 글로벌 엔드포인트가 사용될 수 있습니다.

- Google Cloud 기반 생성형 AI 추론

[1] https://cloud.google.com/docs/security/encryption/default-encryption

- 외부 메일 서비스를 이용한 인증·알림 메일
- 고객이 직접 등록한 외부 API 또는 웹훅

처리 목적, 공급자, 국가와 위탁기간은 개인정보처리방침과 적용 계약에서 안내합니다. “서울 저장”은 모든 일시적 네트워크 처리와 외부 AI 추론이 서울 안에서만 수행된다는 의미가 아닙니다.

5.4 개인정보 마스킹

고객이 개인정보 마스킹을 활성화한 챗봇에는 공통 마스킹 모듈을 적용합니다. 현재 모듈은 지원되는 주요 개인정보 유형을 탐지·마스킹합니다.

마스킹은 운영 로그, 대화 기록과 운영자 조회 등 지원되는 경로에 적용되며, 운영자 조회 시 현재 설정에 따라 기존 데이터도 반환 직전에 다시 보호합니다. 정규식 기반 마스킹은 모든 문맥과 개인정보 유형을 완전하게 탐지하는 DLP 보증이 아닙니다.

5.5 대화 비저장 설정

대화 비저장이 활성화된 챗봇은 다음 동작을 수행합니다.

- 대화 요약과 원문 대화 저장 범위를 축소
- 저장이 필요한 정책 상태에는 원문 대신 대체정보 사용
- 세션 종료 시 첨부 객체와 단기 대화 문맥 정리

이 설정은 대화 본문 저장 경로를 줄이지만, 과금·보안·오류 분석을 위한 운영 및 사용량 기록의 보존정책과 동일하지 않습니다. 고객은 개인정보 마스킹과 대화 비저장 설정의 적용범위를 서비스 설정과 계약 조건에 따라 판단해야 합니다.

5.6 보존과 삭제

데이터 유형	현재 기준
운영·보안 로그	목적, 중요도와 법적·운영상 필요에 따른 보존정책 적용
클라우드 감사로그	공급자의 보호·보존정책과 Cloudturing 접근통제 적용
단기 세션·대화 문맥	제한된 수명과 처리량을 적용하고 세션 종료 정책에 따라 정리
임시 업로드	임시 객체 수명주기 정책과 확인·정리 흐름 적용
고객 파일·업무 데이터	서비스 이용, 고객 삭제 요청, 계약·약관과 법정 보존 요건에 따라 처리

6 애플리케이션과 파일 처리 보안

6.1 서버 측 보안경계

- 서버가 세션 만료, 사용자 상태, 멤버십과 요청 범위를 확인합니다.
- 관리자 전용 작업은 일반 멤버 작업과 구분합니다.
- 저장 콘텐츠와 챗봇 출력은 지원되는 형식별 허용목록으로 정화합니다.
- 불필요한 서버 식별정보를 줄이고 주요 변경 요청의 출처와 콘텐츠 유형을 확인합니다.
- 런타임은 챗봇 운영·결제 상태와 고객 접근정책을 메시지 처리 전에 확인합니다.

6.2 파일 업로드

파일 업로드는 일반 애플리케이션 처리와 분리된 경계를 사용합니다.

- 사용자·챗봇·목적에 제한된 단기 업로드 승인을 검증합니다.
- 서버가 저장 범위와 파일명을 확인하고 비정상 경로를 거부합니다.
- 지원되는 흐름에서 크기, 형식과 실제 콘텐츠 유형을 확인합니다.
- 임시 처리영역과 최종 저장영역을 구분하고, 이미지는 실제 디코딩과 안전한 형식 변환을 적용합니다.

파일 검사 범위

파일 검사는 형식과 사용 목적에 따라 인증, 범위, 크기, 콘텐츠 유형과 안전한 변환을 조합합니다. 검사 항목과 전용 탐지 적용범위는 파일 유형별로 다를 수 있으며, 지원 형식과 개별 제한은 제품 화면과 기술문서의 현재 안내를 따릅니다.

6.3 외부 API와 웹훅

외부 연동은 HTTPS를 기본으로 하고, 공급자 또는 고객 API가 지원하는 요청 서명, 토큰과 사용자 인증을 적용합니다.

AI가 외부 API를 직접 호출 권한으로 사용하는 것이 아니라 애플리케이션 코드가 최종 실행을 담당합니다. 활성화·승인된 도구만 로드하고, 외부 사용자 인증이 설정된 경우 인증 완료 전 사용자 데이터 조회와 사용자 정의 API 실행을 차단합니다.

고객이 관리하는 API 서버의 접근통제, 자격증명 발급과 요청 로그는 고객 책임입니다. Cloudturing은 자사에 저장된 연동 설정, 요청 생성, 민감정보 마스킹과 실행 한도를 관리합니다.

6.4 소프트웨어 변경과 의존성

코드와 인프라 구성은 버전관리합니다. 애플리케이션은 잠금파일과 재현 가능한 빌드 절차로 의존성을 설치합니다. 인증, 권한, 개인정보, 로그 writer, 파일 업로드와 외부 연동에는 서비스별 단위·통합·보안 회귀시험이 존재합니다.

보안검증의 도구와 적용범위는 저장소와 배포경로의 특성에 따라 다르며, 본 백서는 모든 구성요소에 동일한 자동화 검사가 적용된다고 주장하지 않습니다.

7 AI와 RAG 보안

7.1 모델과 실행 책임의 분리

관리자 시스템은 사용 가능한 모델 목록과 운영 상태를 관리하고, 런타임 코드는 공급자 SDK·API, 모델 파라미터, 응답 형식과 도구 호출을 구현합니다. 모델 목록에 항목이 존재한다는 사실만으로 임의 모델을 호출하지 않으며, 실제 호출은 배포된 코드가 지원하는 경로를 사용합니다.

7.2 프롬프트와 도구 실행

사용자 프롬프트, RAG 문서와 외부 API 응답은 비신뢰 데이터로 취급합니다. 중요한 보안경계는 프롬프트 지시문이 아니라 프로그램 코드에 둡니다.

- 승인·활성 상태를 통과한 도구만 모델에 제공합니다.
- 한 요청에서 실행 가능한 도구 호출을 제한합니다.
- 구조화 출력과 서버 측 대상 식별자를 검증하는 경로가 있습니다.
- 인증이 필요한 사용자 데이터와 고객 API 도구는 인증 완료 전 실행하지 않습니다.
- 도구 실행 요약은 민감 키를 마스킹하고 원문 요청·응답을 감사로그에 그대로 복제하지 않습니다.

7.3 RAG 테넌트 격리

점검한 RAG 경로는 서버가 확인한 테넌트 식별자를 논리적 범위로 사용합니다. 업무 데이터, 객체, 로그와 검색 결과에 동일한 범위를 적용하고, 검색 데이터 재구축 시에도 해당 테넌트로 제한된 정본만 사용합니다.

격리 방식

Cloudturing의 기본 격리는 고객·챗봇 식별자와 서버 권한검사에 기반한 논리적 격리입니다. 별도 계약이 없는 경우 고객별 전용 물리환경 제공을 의미하지 않습니다.

7.4 출력 안전성과 추적

지원되는 AI 경로에서 공급자의 완료 · 안전 · 차단 상태를 구분하고, 구조화 응답을 검증합니다. AI 사용기록에는 모델, 사용량, 처리시간, 요청 식별자와 공급자 오류 등 운영에 필요한 메타데이터를 기록합니다.

모델 안전설정은 기능 목적에 따라 다를 수 있으며, 모델의 안전필터만을 유일한 보안경계로 사용하지 않습니다. 권한변경, 외부 발송과 데이터 조회 같은 동작은 애플리케이션 코드의 권한과 입력검증을 통과해야 합니다.

7.5 AI 공급자 데이터 처리

Google Cloud는 고객의 사전 허가 또는 지시 없이 관리형 AI 서비스의 고객 데이터를 모델 훈련이나 미세조정에 사용하지 않는다고 설명합니다. 다만 악용 모니터링, 외부 정보 결합, 세션형 기능 등에는 기능별 보존 조건과 예외가 존재할 수 있습니다. [2]

따라서 본 백서는 모든 AI 기능이 자동으로 "무보존"이라고 주장하지 않습니다. 실제 보존은 사용 기능, Google Cloud 약관과 프로젝트 설정을 함께 적용합니다.

8 감사, 로그와 모니터링

8.1 로그 계층

계층	현재 기록
클라우드 감사로그	관리 활동, 시스템 이벤트와 지원되는 서비스별 감사기록
외부 경계 로그	주요 외부 요청 · 응답 메타데이터
플랫폼 로그	시스템 구성요소와 애플리케이션 워크로드 로그
인증 로그	지원되는 인증 결과와 보안 분석용 메타데이터
애플리케이션 로그	챗봇 설정, 사용량, AI 호출, 웹 위젯, 감사와 크레딧 기록
고객 감사로그	고객이 서버 권한검사 후 자기 챗봇의 주요 변경을 조회 · 검색

8.2 로그 보호와 개인정보

운영 애플리케이션 로그는 분리된 분석 저장소와 보존정책을 사용합니다. 클라우드 감사로그는 공급자의 보호된 감사 계층에 저장됩니다. 개인정보 마스킹이 활성화된 챗봇은 지원되는 로그 처리와 운영자 조회에서 개인정보를 마스킹합니다.

[2] https://cloud.google.com/vertex-ai/generative-ai/docs/vertex-ai-zero-data-retention

감사로그에는 민감한 요청·응답 원문을 불필요하게 복제하지 않으며, 고객 감사로그 조회는 챗봇 멤버십과 조회 범위를 확인합니다. 데이터 접근로그는 서비스 기본 동작과 프로젝트 설정에 따라 범위가 달라지므로, 모든 데이터 읽기 이벤트가 기록된다고 보증하지 않습니다.

8.3 경보와 운영 가시성

현재 모니터링은 다음을 포함합니다.

- 주요 플랫폼·워크로드 상태
- 애플리케이션 오류 조건과 자원 고갈 이벤트
- 실행환경의 용량·수명주기 사건
- 로그·분석 전송 계층의 초기화, 전송 실패와 재연결 상태

경보는 운영 통지 채널로 전달됩니다. 본 백서는 모든 서비스 지표에 24시간 상시 SOC, 외부 합성 모니터링 또는 고객별 탐지규칙이 적용된다고 주장하지 않습니다.

9 가용성, 백업과 복구

9.1 서비스 상태 확인과 자가복구

관리형 외부 경계와 실행환경의 상태 확인을 사용해 서비스 시작, 생존과 요청 처리 가능 상태를 구분합니다. 실행 플랫폼은 비정상 인스턴스를 다시 기동하고, 외부 경계는 정상 처리 대상으로 요청을 전달합니다.

일부 비동기 writer와 사건 처리기는 전송 실패를 구조화 로그로 남기고, 복구 가능한 오류에서 재연결·재시도를 수행합니다.

9.2 업무 데이터 보호

기준일 현재 주요 업무 데이터 저장소에는 다음 보호가 적용됩니다.

- 정기 자동 백업과 내부 보존정책
- 인스턴스 삭제 방지
- 저장공간 자동 확장
- 신원 기반 데이터베이스 인증과 암호화 연결

세션·캐시·검색 데이터는 업무 데이터 정본에서 다시 구성할 수 있는 파생 데이터로 취급합니다.

가용성·복구 보증의 범위

현재 기본 업무 데이터 구성은 정기 백업과 복구 통제를 사용합니다. 특정 복구기능, 가용성, 복구시간, 데이터 손실 한도와 보상은 일률적으로 보증하지 않으며, 고객별 계약·SLA와 실제 기술 구성 및 복구시험의 적용 범위를 따릅니다.

10 보안 운영과 거버넌스

10.1 정책과 문서

Cloudturing은 서비스 약관, 개인정보처리방침, 기술문서와 본 보안백서를 통해 서비스 책임, 개인정보 처리, 위탁 공급자와 주요 보안 통제를 안내합니다. 코드·IaC·운영 설정은 Git과 GCP 실환경을 대조해 관리합니다.

개인정보처리방침에는 처리 항목·목적·보존, 수탁자, 처리 국가와 문의 책임부서를 공개합니다. 본 백서는 개인정보처리방침이나 고객 계약과 충돌할 경우 이를 대체하지 않습니다.

10.2 변경관리

코드와 IaC 변경은 Git 이슈·브랜치·리뷰·테스트·배포 흐름을 사용합니다. 데이터베이스 스키마 변경은 명시적인 마이그레이션과 검증을 요구하고, 운영 인프라의 일부는 실제 권한·연결·비밀정보 상태를 기대값과 비교하는 자동 검증 절차를 제공합니다.

10.3 보안 사건 대응 기반

현재 기술적 대응 기반은 다음을 포함합니다.

- 클라우드 감사, 외부 경계, 플랫폼과 애플리케이션 로그를 이용한 사건 범위 확인
- 고객 감사로그를 통한 챗봇별 주요 변경 추적
- 사용자 전체 세션 회수와 고객 멤버십 정리
- 고객별 네트워크 차단과 보안설정 변경 기록
- 변경이력과 배포기록을 이용한 변경 원인 확인

고객·공공기관에 대한 증거 제공, 사고 통지, 조사 협조와 보존 의무는 적용 법령과 계약에 따라 승인된 범위에서 수행합니다. 다른 고객의 정보, 개인정보와 내부 비밀정보는 제공 범위에서 제외하거나 마스킹해야 합니다.

10.4 공급자와 외부 의존성

주요 공급자 범주에는 Google Cloud와 Google Workspace, 외부 메일·DNS 서비스가 있습니다. Cloudturing은 서비스 목적과 데이터 흐름을 개인정보처리방침과 내부 자산·공급자 자료에서 관리합니다. 고객이 등록한 외부 API는 고객과 Cloudturing의 공동책임으로 운영합니다.

11 고객이 사용할 수 있는 보안 기능

기능	설명	주요 책임
챗봇 멤버 관리	소유자가 멤버 초대·확인·제거	고객 소유자
도메인 접근제한	허용 호스트·하위도메인 기준으로 위젯 연결 통제	고객 설정, Cloudturing 집행
IP/CIDR 접근제한	챗봇별 허용·차단 규칙과 감사기록	고객 설정, Cloudturing 집행
개인정보 마스킹	지원되는 개인정보 유형을 로그·운영자 조회에서 마스킹	고객 활성화, Cloudturing 처리
대화 비저장	요약·원문 대화 저장과 세션 첨부·캐시 범위를 축소	고객 활성화, Cloudturing 처리
감사로그 조회	자기 챗봇의 주요 설정 변경을 검색·조회	Cloudturing 제공, 고객 검토
세션·멤버 회수	운영 관리자 세션 회수와 고객 소유자의 멤버 제거	Cloudturing·고객

고객 보안 운영 권고

- 소유자와 멤버를 정기적으로 검토하고 퇴직·계약종료 사용자를 즉시 제거하십시오.
- 챗봇 용도에 필요하지 않은 개인정보와 비밀정보를 업로드하거나 프롬프트에 넣지 마십시오.
- 외부 API에는 최소권한 자격증명, HTTPS, 짧은 만료와 고객 측 접근로그를 적용하십시오.
- 공개 웹사이트가 아니라면 도메인·IP 접근제한을 활성화하고 변경기록을 검토하십시오.
- 민감한 대화에는 개인정보 마스킹과 대화 비저장 설정의 실제 적용범위를 확인하십시오.

12 준거성과 CSAP 준비 상태

12.1 현재 준거성 자료

Cloudturing은 다음 현재 자료를 보안관리와 고객 설명의 기반으로 사용합니다.

- 서비스 약관과 개인정보처리방침
- 현재 아키텍처·데이터 흐름과 외부 공급자 현황
- 코드·IaC와 GCP 실환경을 대조한 통합 보안 체크리스트
- 고객 감사로그와 운영 로그
- 본 보안백서와 기술문서

12.2 GCP 인증과 Cloudturing의 책임

Google Cloud의 보안 인증과 제3자 감사는 기반 클라우드에 대한 자료입니다. Cloudturing은 GCP의 물리·인프라 통제를 상속할 수 있지만, SaaS 애플리케이션의 인증·권한·데이터 흐름·설정·로그·복구와 고객 계약은 Cloudturing의 책임입니다.

따라서 "GCP가 인증을 보유한다"는 사실을 "Cloudturing SaaS가 동일 인증을 취득했다"는 의미로 사용하지 않습니다.

12.3 CSAP 준비 고지

Cloudturing은 CSAP 취득 준비 활동을 진행 중입니다. 현재 활동에는 보안관리 범위와 자산·데이터 흐름 식별, 통제 타당성 검토, 코드·인프라 현황 대조, 현재 보안백서와 내부 개선자료 정비가 포함됩니다.

비보증

본 백서는 CSAP 인증서가 아니며, 인증 신청의 최종 등급·범위·제외 항목, 평가 결과 또는 인증 취득을 보장하지 않습니다. 공공기관은 실제 인증상태, 적용 업무 중요도, 계약범위와 기관 자체의 보안성·적합성 절차를 별도로 확인해야 합니다.

13 해석상 유의사항

1. **시점성:** 본 문서는 2026년 7월 31일 현재 코드와 클라우드 설정 점검을 기반으로 합니다. 서비스 구성은 보안·운영 필요에 따라 변경될 수 있습니다.
2. **공개 범위:** 비공개 도메인, 시스템 식별자, 세부 토폴로지와 탐지 임계값은 공개하지 않으며

필요 시 적법한 비밀유지 절차에서 별도 확인합니다.

3. **범위성**: 기술 통제는 기능, 고객 설정, 데이터 유형과 계약 범위에 따라 적용 여부가 달라질 수 있습니다.
4. **논리적 격리**: 기본 테넌트 격리는 식별자·권한검사와 데이터 범위를 이용한 논리적 격리이며 별도 계약 없는 고객별 물리 인프라 제공을 의미하지 않습니다.
5. **AI 처리**: AI 기능의 처리지역·보존은 사용 모델·기능과 공급자 약관을 함께 적용합니다.
6. **가용성**: 백업과 자가복구 통제는 존재하지만, 별도 계약 없이 특정 복구목표나 무중단을 보증하지 않습니다.
7. **고객 책임**: 사용자·멤버, 업로드 데이터, 외부 API, 최종 이용자 단말과 고객 네트워크는 고객이 통제해야 하는 보안영역입니다.

14 부록

14.1 용어

용어	설명
CSAP	클라우드서비스 보안인증제
IAM	Identity and Access Management, 신원·권한 관리
RAG	검색 결과를 생성형 AI 입력 문맥에 결합하는 방식
PII	개인을 식별하거나 식별 가능하게 하는 정보
PITR	Point-in-Time Recovery, 특정 시점 복구
RTO/RPO	복구 목표시간 / 허용 가능한 데이터 손실 시점
SLA	서비스 수준 합의
SSRF	서버가 공격자가 지정한 내부·외부 목적지로 요청하게 만드는 공격
TTL	데이터 또는 캐시의 유효기간

14.2 공식 참조자료

1. Google Cloud, **Default encryption at rest**
   https://cloud.google.com/docs/security/encryption/default-encryption
2. Google Cloud, **Generative AI data governance**

https://cloud.google.com/vertex-ai/generative-ai/docs/vertex-ai-zero-data-retention

3. 한국인터넷진흥원, **클라우드서비스 보안인증제 제도소개**
https://isms.kisa.or.kr/main/csap/intro/index.jsp

14.3 문서 이력

버전	날짜	변경 내용
1.0	2025-12-15	최초 작성
1.1	2025-12-16	기반 인프라 보안정책과 업데이트 설명 보완
2.0	2026-07-31	코드·IaC·GCP 실환경 점검을 반영해 현재 통제 중심으로 전면 개정. CSAP 준비 비보증, 공동책임, 테넌트·AI·파일·로그·복구 경계를 명확화
2.1	2026-07-31	공개본에서 비공개 도메인, 내부 식별자, 세부 토폴로지·보존값·탐지 기준을 통제 목적과 보호 방식 중심으로 범주화

Cloudturing

보안 백서 문의: cto@cloudturing.com