ERICSSON

공급자 정보 보안 요구 사항

ISRS

Security Requirements

소개

Ericsson 공급자 정보 보안 요구사항(Ericsson Information Security Requirements for Suppliers)("요구사항")은 공급자가 아래에 해당하는 상황에서 모든 공급자 관계에서 반드시 준수해야 하는 최소 수준의 정보 보안 요구 사항을 정하고 있습니다.

1. Ericsson 정보를 처리, 저장 및/또는 접근합니다.
2. Ericsson 네트워크/인프라에 접근할 수 있습니다.
3. Ericsson을 위해 소프트웨어를 개발하고 맞춤화합니다.
4. 지원 및 유지관리 서비스와 함께 IT 하드웨어 또는 소프트웨어 제품을 제공합니다.

요구 사항은 정보 보안 요구 사항의 전체 목록이 아닙니다. 본 요구 사항 외에도, 공급되는 각 서비스별로 적절한 정보 보안 통제 장치를 통해 대응해야 하는 구체적인 요구 사항이 필요할 수 있으며, 이러한 통제 장치에 대해서는 관련 계약서에서 자세히 정의합니다.

이 문서는 정기적으로 검토되며 수시로 업데이트됩니다.

목차

1 정보 보안 요구 사항

공급자는 최신 버전의 국제 표준 ISO/IEC 27001 또는 서면 합의에 따른 동등한 표준을 준수하여 정보 보안 관리에 대한 체계적인 접근 방식을 입증해야 합니다.

1.1 정보 보안 관리

a. 공급자의 최고 경영진은 반드시 정보 보안에 대한 방향을 설정하고 실행 의지를 입증해 보여야 합니다. 최소한, 전사적 차원에서 적용되는 높은 수준의 정보 보안 정책과 지원 프로그램이 있어야 합니다.

b. 위의 a.항에 따른 정보 보안 정책은 반드시 공급자의 경영진에 의해 승인되어야 하며, 공급자 조직 내에 게시되고 공급자의 관련 직원들에게 전달되어야 합니다.

c. 공급자의 정보 보안 정책은 지속적인 적합성, 타당성 및 효과를 보장할 수 있도록 최소 이십사(24) 개월마다 1회 이상의 사전에 계획된 주기로, 또는 중대한 변경 사항이 발생하는 경우 반드시 검토해야 합니다.

d. 정보 보안 프로그램을 유지할 책임이 있는 한 명 이상의 자격을 갖춘 인원이 반드시 지정되어야 합니다.

e. 공급자는 보안상 안전한 근무 환경을 조성하고 유지하기 위한 직원의 책임에 대해 교육하기 위해서 정기적으로 정보 보안 의식 캠페인을 실시합니다.

f. 공급자는 해당하는 경우 반드시 적절한 업무 분리를 유지해야 합니다.

1.2 위험 관리

공급자는 반드시 정보 보안 리스크를 식별 및 대응할 수 있도록 위험 관리 체계/절차를 갖추고 있어야 합니다.

1.3 인적자원 보안

a. 공급자는 반드시 관련 법률에 따라 공급자의 모든 직원에 대해 채용 전 신원 검증 확인을 실시해야 합니다. 이러한 신원 확인의 증거는 반드시 보관하고 (Ericsson이 요청 시) Ericsson에 제공해야 합니다.

b. 공급자의 직원은 Ericsson 정보에 대한 접근 권한을 얻기 전에 기밀 유지 의무를 위해 반드시 해당 공급자와의 서면 동의서를 체결하여야 합니다(예: 직원 동의서 또는 NDA[기밀 유지 서약서]). 이러한 기밀유지계약은 공급자 직원이 Ericsson 정보를 제3자에 제공하는 것을 금지해야 하며, 공급자가 Ericsson과 체결한 계약에 대한 기밀 유지 의무와 최소 동일한 수준을 유지하여야 합니다.

c. Ericsson 네트워크 인프라 및/또는 Ericsson 정보에 대한 접근 권한을 보유하고 있는 공급자의 직원은 반드시 Ericsson의 기밀 유지 및 접속에 관한 지침(Non-Disclosure and Access Instruction) 문서(NDI)에 서명해야 합니다.

d. 공급자는 정보 보안 위반에 대응하기 위한 징계 절차를 갖추고 있어야 합니다.

1.4 자산 관리

a. 공급자는 Ericsson 정보를 기밀 정보로 취급하고 본 문서에 명시된 요구 사항을 준수하여 이를 보호해야 합니다.

b. 공급자는 반드시 서비스의 일부인 정보 기술 자산을 등록하고 그 보유 내역을 유지 관리해야 합니다.

c. 공급자는 계약에 따른 의무를 이행하는 것 외에는 다른 목적으로 Ericsson 정보를 저장, 인쇄, 복사, 공개 또는 처리해서는 안 됩니다.

d. 공급자는 공급자의 직원을 해고하거나 그 고용을 변경할 경우 Ericsson 자산 반환에 대한 절차를 수립해야 합니다.

e. 공급자는 업계 모범 사례에 따라 Ericsson 정보를 안전하게 삭제하기 위한 절차를 수립하고 유지해야 합니다(재사용이 가능해지기 전에 전자 매체에서 삭제하는 경우 포함).

f. Ericsson과의 계약이 종료 또는 해지되는 경우, 공급자는 모든 백업 및 기록용 보관 사본을 포함하여 공급자가 보유하고 있는 일체의 모든 전자적 또는 비전자적 형태의 Ericsson 정보의 모든 사본을 반드시 업계 모범 사례에 따라 반환하거나 안전하게 파기해야 합니다. 요청 시, 공급자는 Ericsson에게 서면 확인서 또는 파기 인증서를 제공해야 합니다.

1.5 접근 통제

a. Ericsson의 통제 밖에 있는 네트워크에서 Ericsson의 일원이 아닌 개인 또는 단체가 Ericsson 자산에 접근하는 것은 승인된 Ericsson 원격 접근 솔루션을 통해서만 허용됩니다.

b. Ericsson 정보에 대한 접근은 반드시 특정 개인으로 한정하고 알 필요가 있는 경우로 제한되어야 합니다.

c. 계정 공유는 엄격히 금지합니다. Ericsson 정보에 접근하는 각 개인은 자신만의 고유한 계정을 보유해야 합니다.

d. Ericsson 정보가 포함된 시스템 및 네트워크에 대한 모든 접근에는 업계 표준 모범 사례에 따라 다중 인증(MFA)을 구현해야 합니다.

e. 공급자는 Ericsson 정보에 접근할 때 비밀번호 복잡성, 허용되는 최대 로그인 실패 횟수, 비밀번호 만료 기간 등을 포함하여 업계 모범 사례에 따라 비밀번호 설정 및 관리 통제를 구현해야 합니다.

f. 공급자는 Ericsson 정보를 처리, 전송 또는 저장하는 자사 네트워크 및 시스템에서 사용자를 추가, 변경 또는 삭제하는 경우 반드시 승인을 받도록 하는 절차를 보유해야 합니다.

g. 공급자는 고용 종료 또는 직원 변경 시 접근 권한을 철회/업데이트하는 절차를 반드시 보유해야 합니다.

h. 공급자는 관리자 접근 권함을 포함하여 Ericsson 정보를 처리하는 시스템 및 네트워크에 대한 접근 권한을 검토해야 합니다. 정기적인 권한 검토는 최소 십이(12) 개월마다 수행되어야 하며, 특별 권한을 보유한 사용자의 경우 최소 삼(3) 개월마다 검토가 이루어져야 합니다.

i. 공급자는 반드시 특별 권한이 있는 계정을 관리하고 운영하는 절차를 보유해야 합니다.

j. 기록은 반드시 어떠한 Ericsson 정보가 접근, 수정, 공개 또는 폐기되었는지를 확인할 수 있는 방식으로 보관되어야 합니다.

1.6 암호화

a. 암호화 통제는 모든 관련 계약, 법률 및 규정을 준수하여 구현되어야 합니다.

b. 공급자는 Ericsson과의 안전한 통신을 위해 반드시 업계 표준 모범 사례 암호화 기술을 사용해 암호화한 이메일을 사용해야 합니다.

c. Ericsson 정보의 보호를 위해 공급자는 업계 표준 모범 사례에 따른 암호화 기술을 사용하여 전송 및 저장해야 합니다.

d. 암호화 키는 업계 표준 모범 사례에 따라 키 생성, 갱신, 접근, 배포, 저장, 보관, 폐기 및 파기를 위한 절차를 갖춘 중앙 집중식 관린 체계로 운영되어야 합니다.

e. 루트 인증서는 운영 환경에서는 절대 사용하지 않습니다.

1.7 물리적 및 환경적 보안

a. 공급자는 Ericsson 정보가 처리되거나 저장되는 시설 및 데이터 센터에 대한 물리적 접근을 최소한의 인원으로 제한하고 필요에 따라 접근 권한을 부여해야 합니다.

b. Ericsson 정보가 처리되는 정보 처리 시설은 연중무휴(24시간X7일) 모니터링 및 접근 통제가 이루어져야 합니다.

c. 공급자는 Ericsson 정보가 처리되는 정보 처리 시설을 외부 및 환경적 위협과 위험으로부터 보호해야 합니다.

d. Ericsson의 정보 및 자산을 보호하기 위해 깨끗한 책상 및 화면 잠금 정책(Clear desk and Clear screen policy)을 시행해야 합니다.

e. Ericsson을 위한 서비스가 수행되는 장소에 대한 물리적 접근은 개별 스와이프/근접 카드 또는 이에 상응하는 시스템을 사용하여 제한해야 합니다.

f. Ericsson을 위한 서비스가 수행되는 장소에 대한 물리적 접근이력(날짜, 시간, 스와이프/근접 카드 ID, 출입문 ID, 접근 거부 또는 접근 허가 등)을 지속적으로 기록해야 합니다.

1.8 운영 보안

a. 공급자의 시스템에는 보안 사고나 수요 증가가 발생하는 경우에도 지속적인 가용성을 보장할 수 있는 충분한 용량으로 구성되어야 합니다.

b. 공급자는 업계 표준 모범 사례에 따라 자체 시스템 내에 악성 소프트웨어 방지 솔루션을 배포하고 최신 상태로 유지해야 합니다.

c. 모든 권한이 있는 사용자의 작업은 반드시 기록(로그)되어야 하며, 시스템 사용자, 권한 있는 사용자 또는 최종 사용자가 이러한 로그를 수정할 경우 반드시 탐지 가능해야 합니다. 또한 로그 기록을 반드시 주기적으로 독립적인 검토를 거쳐야 합니다.

d. 중요 보안 이벤트 (예: 로그온 실패, 시스템 충돌, 접근 권한 변경)는 날짜, 시간, 사용자 ID, 파일명, 사용자 활동 유형, IP 주소 등의 속성과 함께 기록되어야 합니다.

e. 로그 기록은 반드시 최소한 육(6) 개월 동안 암호화된 상태로 저장되어야 하며, 요청 시 Ericsson에 제공되어야 합니다.

f. 계약상의 연속성과 제공 기대치를 충족하기 위해 반드시 정기적인 백업을 수행하고 유지해야 합니다.

g. 취약점의 특성/심각도에 따라 취약점의 우선순위를 정하고 이를 개선하기 위한 취약점 관리 절차를 반드시 수립해야 합니다.

h. 패치를 적시에 적용하기위한 패치 관리 절차를 구축해야 합니다.

i. 공급자는 Ericsson 연계 시스템 및 인프라에 대해 업계 표준 모범 사례를 준수한 최소 연 1회침투 테스트를 실시해야 합니다.

j. 공급자는 모든 관련 정보 처리 시스템의 시계를 단일 기준 시간 소스에 동기화 해야 합니다.

k. 공격 표면을 줄일 수 있도록 모든 시스템에 대해 현행 업계 표준 모범 사례에 따른 시스템 강화 조치(Hardening)를 적용해야 합니다.

l. 공급자는 Ericsson의 사전 서면 동의 없이 휴대용 기기에 Ericsson 정보를 저장하는 것을 방지하는 정책을 구현해야 합니다.

m. 공급자는 반드시 적절한 물리적, 기술적 및/또는 논리적 수단을 사용해 Ericsson 정보 및 애플리케이션/시스템이 공급자 자체 또는 타 고객 시스템과 분리되도록 보장해야 합니다.

n. Ericsson 정보가 포함되어 있는 개발, 테스트 및 운영 환경은 반드시 서로 논리적 및 물리적으로 분리되어 있어야 합니다.

o. 공급자는 계약서에 별도로 명시되지 않은 경우에는 Ericsson 정보를 어떠한 인공지능(AI)에서 사용해서는 안 됩니다.

1.9 통신 보안

a. 공급자는 사용하지 않는 소프트웨어 및 기능을 제거하거나 비활성화 하는 방식을 포함하여 Ericsson 정보가 포함된 시스템을 업계 표준 모범 사례에 따라 강화하여야 한다.

b. 공급자는 Ericsson 정보를 보호하기 위해서 업계 표준 모범 사례에 따라 보안이 강화된 방화벽, 침입 탐지/방지 시스템, 네트워크 분할 및 기타 관련 조치를 활용하여 다층적 보안 접근 방식을 구현해야 합니다.

c. 공급자는 맬웨어, 이메일 스푸핑, 피싱 공격, 스팸과 같은 악의적인 공격으로부터 보호하기 위해 업계 표준 모범 사례에 따라 이메일 보안 솔루션을 구현해야 합니다.

1.10 협력업체 관계

a. 협력업체에 Ericsson의 정보를 공개하는 것은 Ericsson의 사전 서면 동의가 있는 경우에만 허용되며, 계약에 따라 공급자의 의무를 이행하는 목적으로만 허용됩니다.

b. 협력업체는 계약상의 의무를 이행하는 데 필요한 Ericsson 정보만 접근, 사용, 보관 및 공개하여야 한다.

c. 공급자는 서면 계약을 통해 본 문서에 명시된 것과 동일한 의무 사항을 협력업체에게 전달할 책임이 있습니다.

d. 공급자는 새로운 협력업체와 계약하기 전에 반드시 해당 업체에 대해 위험 평가를 실시해야 하며 제3자 위험 관리 절차를 갖추고 있어야 합니다.

e. 공급자는 요구 사항에 대한 협력업체의 준수 여부를 정기적으로 모니터링, 검토 및 감사를 진행해야 합니다.

1.11 사고 관리

a. 공급자는 반드시 사고를 감지 및 처리할 수 있도록 문서화된 보안 사고 관리 절차를 갖추고 있어야 합니다.

b. 공급자는 Ericsson 정보에 영향을 미치는 사고를 인지하는 즉시 Ericsson에 그 사실을 통보해야 합니다. 해당 통보는 실제 사고가 발생했거나 발생이 의심되는 사고에 대해 인지하게 된 시점으로부터 늦어도 이십사(24) 시간 이내, 또는 달리 합의된 기한 내 다음 연락처로 고지되어야 합니다.

   i. 계약서에 명시된 Ericsson 담당자, 그리고

   ii. gs.sim.dispatch@ericsson.com

c. 모든 보안 관련 사고에 대한 보고는 기밀 정보로 취급하고 업계 표준 모범 사례에 적용된 암호화 방법을 사용하여 암호화해야 합니다.

d. 공급자는 이러한 보고를 처리할 때 반드시 Ericsson에 전적으로 협조해야 합니다. 협조에는 포렌식 평가를 위해 컴퓨터 기반 증거 데이터에 대한 접근을 제공하는 것이 포함될 수 있습니다.

e. 공급자는 Ericsson과 협력하여 서비스에 영향을 미치거나 Ericsson 정보와 관련된 보안 사고나 취약점에 대한 시정 조치의 일환으로 상호 합의된 적절한 보안 조치 및 절차를 구현하도록 해야 합니다.

1.12 사업 연속성 관리

a. 공급자는 연간 테스트되고 문서화된 사업 연속성 및 재난 복구 계획을 수립해야 하며, Ericsson의 요청 시 해당 계획의 사본을 제공해야 합니다.

b. 공급자는 정보 보안 및 ICT 준비 요구 사항이 사업 연속성 및 재난 복구 계획에 포함되어 있는지 확인해야 합니다.

c. Ericsson의 요청 시 공급자는 반드시 Ericsson이 지정하는 바에 따라 상호 사업 연속성 및 재난 복구 활동에 기여해야 합니다.

1.13 시스템 취득, 개발 및 유지관리

Ericsson 정보의 처리를 포함해 소프트웨어 또는 하드웨어 개발 또는 맞춤화(customization) 서비스를 제공하는 공급자는 다음 정보 보안 요구 사항을 준수해야 합니다.

a. 공급자는 문서화된 소프트웨어 개발 수명 주기(SDLC) 방법론을 보유해야 합니다.

b. 시스템 소스/개체 코드는 무단 접근으로부터 보호되어야 하며, 소스 코드 저장소에 대한 접근 권한은 주기적으로 검토되고, 권한이 있는 직원으로 접근 권한을 한정해야 합니다.

c. 생산 시스템에서의 Ericsson 정보는 테스트 및 개발 시스템에 사용되어서는 안 됩니다.

d. 공급자는 Ericsson 정보를 처리하는 소프트웨어 및/또는 기타 제품이 알려진 보안 취약점 또는 결함이 없도록 보장해야 합니다.

e. Ericsson이 요청 시, 공급자는 Ericsson 정보 처리를 지원하는 소프트웨어 개발에 사용된 모든 제3자 소프트웨어/플러그인(특허 등록된 또는 오픈 소스)을 반드시 공개해야 합니다.

f. 공급자는 애플리케이션 및 인프라 관련 변경요청, 테스트 및 승인을 위한 문서화된 변경 관리 절차를 따라야 합니다.

1.14 소프트웨어 공급망 보안

공급자는 Ericsson에 공급되거나 제공된 모든 소프트웨어(독립형 또는 하드웨어에 내장된 형태로)에 대해 사용된 타사 소프트웨어 구성요소 및 그 각각의 버전 번호(오픈 소스와 특허 등록된 구성요소 모두 해당)를 명시 및 문서화하고, SPDX 사양 V2.2.1/ISO 5962:2021 및 SBOM 공급자 사양(*조건 및 지침 - 공급자 & 파트너 - Ericsson 참조)*에 부합하는 소프트웨어 구성요소 명세서(SBOM)를 Ericsson에 제공하여야 합니다.

2 규정 준수 의무

a. 공급자는 교육을 받은 공급자 직원 또는 공급자가 지정한 제3자로 하여금 정보 보안에 관한 내부 감사 및/또는 평가를 정기적으로 수행하게끔 해야 하며, 발견된 문제는 즉시 수정해야 합니다.

b. Ericsson 요청 시, 공급자는 십(10) 일 이내에 본 요구 사항 및 기타 Ericsson과 합의된 정보 보안 요구 사항의 준수 여부를 증명하여야 하며, 확인된 미 준수 사항은 Ericsson에 추가적인 비용 청구 없이 즉시 시정해야 합니다.

c. 공급자는 Ericsson의 요청에 따라 협력업체가 이러한 요구 사항을 준수하고 있다는 증거를 Ericsson에 제공해야 합니다.

d. Ericsson의 요청 시, 공급자는 Ericsson의 정보가 처리되거나 저장되어 있는 공급자가 관리 또는 호스팅하고 있는 시스템에 대해 Ericsson이 직접 침투 및/또는 취약점 테스트를 실시하도록 허용하거나 해당 테스트의 결과를 Ericsson에 제공해야 합니다.

e. 공급자는 요구 사항 준수 사실을 입증하기 위해 필요한 모든 기록을 보관하고 보호해야 합니다.

3 정의

본 문서의 목적을 위해, 문맥상 달리 해석해야 하는 것이 분명한 경우를 제외하고, 다음 단어 및 표현은 반드시 아래에서 정하는 의미로 해석해야 합니다.

계약(서)	공급자와 Ericsson 사이의 계약으로, Ericsson이 공급자로부터 제품(소프트웨어 및 기타 지적 재산권으로 보호되는 제품 포함), 서비스 또는 기타 결과물을 구매, 라이선스 제공 또는 임대하는 계약으로 본 요구 사항이 적용됩니다.
신원 검증 확인	신원 검증 확인은 ISO/IEC 27001/27002에서 정하는 것과 동일한 의미를 갖습니다.
Ericsson 정보	Ericsson, Ericsson의 고객, Ericsson과 비즈니스 관계를 맺고 있는 제3자 및 서비스의 일부인 기타 정보에 대한 정보. Ericsson 정보는 개인 정보를 포함합니다.
업계 표준 모범 사례	동일하거나 유사한 상황에서 (해당되는 경우) 수령자 또는 계약자와 동일한 유형의 사업에 종사하는 숙련되고 유능한 서비스 공급자에게 일반적이며 합리적으로 기대되는 수준의 기술, 주의 및 통찰력과 운영 관행을 의미합니다.
정보 처리 시설	Ericsson 정보를 처리하거나 저장하는 시스템이 있는 모든 물리적 장소.
개인 정보	개인 정보는 식별되었거나 식별이 가능한 자연인('데이터 주체')과 관련될 수 있는 모든 정보, 또는 법률, 규정 또는 계약 합의에 따라 정의된 모든 정보를 의미합니다. 식별 가능한 사람이란 이름, 식별 번호, 위치 데이터, 온라인 식별자 또는 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 정체성과 관련된 하나 이상의 특정 요소를 참조함으로써 특히 직접 또는 간접적으로 식별될 수 있는 사람을 말합니다.
서비스	계약에 따라 공급자가 Ericsson에 공급하는 모든 서비스, 제품 또는 기타 결과물을 의미합니다.

단일 참조 시간 소스	전 세계적으로 시계 및 시간을 규정하는 데 사용되는 일차적 시간 표준인 UTC(협정 세계시)의 신뢰할 수 있는 소스에 직접 연결되어 있는 시간 서버 소스(예: Stratum 1)를 의미합니다.
공급자	Ericsson과 계약을 체결하고 서비스를 제공할 회사를 의미합니다. 공급자라는 용어가 본 문서에 따라 공급자에 의무 사항 또는 요구 사항을 부과하는 경우 그러한 용어에는 공급자의 계열사, 협력업체 및 직원이 포함됩니다.