제너릭IT · Generic IT Corporation

보안점검부터 오래된 레거시 시스템까지, 안전하게 고치고 매달 지킵니다

보안점검 대응 · 레거시 시스템 유지보수 전문 개발사

회사소개서 2026

(주)제너릭아이티 | www.genericit.co.kr

보안점검 대응 | 레거시 유지보수 | 보안 운영

COMPANY

회사 소개

고객사의 보안 강화 요구에 대응하고, 만든 업체와 연락이 끊긴 오래된 시스템도 직접 분석해 이어받아 운영합니다. 대기업 · 보험사 · 금융사 보안점검을 대응하고 고객 시스템을 직접 운영해 온 개발팀이 처음부터 끝까지 맡습니다.

회사명	(주)제너릭아이티
대표이사	강덕훈
설립일	2021년 4월 20일 (법인 2021년 12월)
본사	경기도 남양주시 다산순환로 20 현대프리미엄 캠퍼스 A동
전문분야	보안점검 대응 · 레거시 시스템 유지보수 · 보안 운영 · 시스템 구축
인증	혁신성장벤처기업 인증, 기술보증기금 기술평가 통과
사업자등록번호	238-86-02252
팀 구성	CEO · CTO 15년차 풀스택 개발자를 중심으로 17년차 풀스택, 11년차 · 6년차 개발자와 경영지원으로 구성된 개발팀

8 회
보안점검 · 이행점검 대응

22 건
지적 사항 조치 개발

10 개사+
홈페이지 · 시스템 운영 · 유지보수 중

200 +
점검표 항목 대응

2021년 설립 이후 시스템 구축부터 **보안점검 대응**, **레거시 시스템 유지보수**까지 꾸준히 성장하고 있습니다. 2021년 설립 이후 누적 매출 **30억 원**.

PROBLEM

이런 상황, 혼자 해결하기 어렵습니다

보안점검은 문서만 고쳐서는 통과할 수 없고, 점검이 끝난 뒤 관리하지 않으면 다음 점검에서 같은 지적을 받습니다.

“거래하는 대기업에서 보안점검 체크리스트가 왔어요”

항목은 수십 개, 기한은 몇 주. 2단계 인증, 계정 잠금, 암호화, 접속기록 보관까지 무엇이 미흡한지, 어떻게 증명해야 하는지부터 막막합니다.

“지적 사항은 받았는데 개발할 사람이 없어요”

오래전에 외주로 만든 시스템은 소스를 아는 사람이 없습니다. 기능 하나 고치려다 다른 곳이 깨질까 걱정입니다.

“만든 업체와 연락이 안 돼요”

10년 넘은 시스템은 문서도 없고 구조도 낯설어 다른 업체가 손대기를 꺼립니다. 보안 패치도 계정 관리도 멈춘 상태입니다.

“PHP · Java · 서버 OS 지원이 끝났다는데요?”

지원이 끝난 언어 · 프레임워크 · 서버는 보안 패치를 받을 수 없습니다. 점검에서도, 실제 해킹에서도 가장 먼저 문제가 됩니다.

SCOPE

고객사가 요구하는 보안, 고객 정보를 다루는 모든 시스템이 대상입니다

대상 시스템	주요 점검 · 조치 항목	대상 시스템	주요 점검 · 조치 항목
홈페이지 · 쇼핑몰	회원 정보 암호화, 관리자 페이지 접근 제한, 웹 취약점 · 웹셸 점검	**관리자 페이지**	2단계 인증, 로그인 실패 잠금, 접속 IP 제한, 접속기록 보관
ERP · 그룹웨어 · 사내 시스템	1인 1계정, 권한 최소화, 퇴사자 계정 정리, 권한 변경 이력	**고객 · 영업관리 시스템**	개인정보 마스킹, 다운로드 통제, 업무 종료 개인정보 파기
모바일 앱 · API	전송 구간 암호화, 인증 토큰 관리, 불필요한 외부 접근 차단	**서버 · DB · 클라우드**	DB 암호화 · 암호키 분리, 보안 업데이트, 백신, 원격 접속 통제

SERVICES

핵심 서비스 — 세 가지에 집중합니다

점검을 한 번 대응하고 끝나지 않도록, 오래된 시스템을 안전한 상태로 고치고 매달 유지하며 기록합니다.

01 · SECURITY AUDIT

협력업체 보안점검 대응

대기업 · 금융사 · 공공기관 등 고객사의 점검표를 항목별로 분석하고, 홈페이지부터 사내 시스템 · 서버까지 미흡한 부분을 직접 구현합니다.

- 점검 체크리스트 항목별 현황 진단
- 미흡 항목 조치 개발 (인증 · 권한 · 암호화 · 로그 · 파기)
- 항목별 증적 캡처와 회신서 작성 지원
- 재점검 · 보완 이행점검 대응

결과물 조치 완료 시스템 · 증적 자료 · 회신서

02 · LEGACY MAINTENANCE

레거시 시스템 유지보수

만든 업체가 문을 닫았거나 연락이 끊긴 오래된 시스템도 언어와 상관없이 직접 분석해 이어받고, 보안 지원 버전으로 옮겨 계속 운영합니다.

- PHP · Java · ASP · .NET 레거시부터 최신 시스템까지
- 다른 업체가 개발한 시스템 분석 · 인수
- 언어 · 프레임워크 · 서버 OS 보안 업그레이드
- 서버 이관 및 운영 비용 절감

결과물 인수 완료 시스템 · 업그레이드 · 운영 문서

03 · SECURE OPERATION

보안 운영형 유지보수

장애 대응만 하는 유지보수가 아니라, 점검 기준에 맞는 보안 상태를 매달 유지합니다.

- 월간 접속기록 점검 보고서
- OS · 서버 백신 보안 업데이트 관리
- 장기 미접속 · 퇴사자 계정 정리
- 백업 · 장애 대응 · 기능 개선

결과물 월간 점검 보고서 · 운영 기록

보안 컨설팅 · 진단 업체가 문제를 찾아 보고서를 드린다면, 제너릭아이티는 지적 사항을 **실제 운영 시스템의 코드 · DB · 서버에 개발로 조치**하고 증적 · 회신서, 이행점검, 이후 월간 보안 운영까지 맡는 **개발사**입니다.

01 · SECURITY AUDIT

보안점검 대응 — 점검표 분석부터 재점검까지

대기업 · 금융사 · 공공기관은 업무를 맡긴 협력업체(위탁업체, 수탁사)의 보안 수준을 매년 점검하고 보완을 요구합니다. 수탁사 점검 체크리스트는 대부분 「개인정보의 안전성 확보조치 기준」을 바탕으로 하며, 자주 지적되는 항목을 실제 시스템에 구현한 경험이 있습니다.

점검 단계	협력업체가 해야 할 일
사전 질의서	현황 파악, 항목별 답변 작성
서면 · 현장 점검	화면 · 설정 증적 캡처, 시연
지적 사항 통보	조치 계획 수립, 기능 개발
이행점검	조치 결과 증적, 회신서 작성

점검표 양식은 고객사마다 다릅니다. 같은 내용도 묻는 방식과 요구하는 증적이 달라 항목마다 현황을 다시 확인하고 답변을 새로 작성해야 합니다.

계정 · 권한

- 1인 1계정, 최소 권한
- 3개월 장기 미접속 계정 자동 차단
- 퇴사자 계정 삭제 · 권한 변경 이력

안전한 로그인

- 로그인 문자 인증(2단계 인증)
- 5회 실패 시 잠금, 본인 확인 후 해제
- 비밀번호 규칙 · 90일 변경

접근 통제

- 관리자 등록 IP 외 접속 차단
- 웹방화벽 · SSH 무차별 대입 차단
- 동시 접속 제한 · 세션 자동 종료

저장 · 전송 암호화

- 개인정보 DB 암호화
- 첨부파일 · 에디터 본문 암호화
- 암호키 분리, 전송 구간 TLS 1.3

접속기록

- 계정 · 일시 · IP · 수행 업무 기록
- 장기 보관 및 관리자 조회 화면
- 월간 접속기록 점검 보고서

파기 · 악성코드 방지

- 업무 종료 개인정보 파기 기능
- 서버 백신 · OS 보안 업데이트
- 웹셸 · 테스트 파일 제거

02 · LEGACY MAINTENANCE · 03 · SECURE OPERATION

레거시 유지보수 · 보안 운영 — 고장 날 때만 고치지 않습니다

다른 업체가 만든 오래된 시스템도 이어받아, 보안점검 기준에 맞춘 상태를 매달 확인하고 기록으로 남겨 다음 점검 때 그대로 증적으로 쓸 수 있게 운영합니다.

01
인수 분석
어떤 언어든 문서가 없어도 소스 · DB · 서버를 직접 분석

02
보안 업그레이드
지원 종료 런타임을 보안 지원 버전으로 옮기고 깨지는 코드 수정

03
서버 이관
노후 서버를 안전하고 운영 비용이 적은 환경으로 이전

04
계속 운영
월간 보안 점검 · 장애 대응 · 기능 개선

구분	일반 유지보수	보안 운영 유지보수
장애 대응	요청 시 수정	요청 시 수정 + 원인 분석 기록
접속기록	쌓이기만 함	매월 점검 보고서 작성, 이상 징후 판정
계정 관리	요청이 있을 때만	장기 미접속 · 퇴사자 계정 매월 정리
보안 업데이트	문제가 생기면	OS 패치 · 서버 백신 · 웹방화벽 상태 매월 확인
보안점검	별도 대응 필요	쌓인 운영 기록으로 증적 · 회신서 준비

매월

- 접속기록 월간 점검 보고서 (접속 · 다운로드 · 출력 현황, 이상 징후 판정)
- 장기 미접속 · 퇴사자 계정 차단, 권한 변경 이력 확인
- OS 보안 패치, 서버 백신, 웹방화벽 차단 로그 점검
- DB · 첨부파일 백업과 복구 가능 여부 확인

상시 · 연 1회 이상

- 운영 개발팀이 직접 장애 원인 분석 · 수정, 기능 개선
- 고객사 보안점검 대응, 지원 종료 버전 점검 · 런타임 업그레이드

TECHNOLOGY

대응 가능한 기술 — 언어 · 환경과 상관없이 맡습니다

레거시부터 최신 시스템까지, 만든 업체와 연락이 끊긴 시스템도 직접 분석해 보안 조치와 업그레이드를 진행합니다.

구분	대상	주로 하는 작업
Java · JSP	JSP · Servlet, JSTL, Struts 1 · 2, iBatis · JDBC 직접 호출	구조 분석, 취약 코드(SQL 인젝션 · XSS) 수정, 보안 기능 추가
Spring	Spring 3 · 4 · 5 MVC, 전자정부 표준프레임워크 2.x · 3.x · 4.x, MyBatis	프레임워크 버전 업, 라이브러리 교체, 기능 개선
Spring Boot	Spring Boot 2.x · 3.x, JPA · QueryDSL, Spring Security	운영 · 장애 대응, 2.x → 3.x 전환, 인증 · 권한 보강
Java · WAS · 빌드	Java 6 ~ 21, Tomcat / Ant · Maven · Gradle, 수동 WAR 배포	JDK · Tomcat 지원 버전 전환, WAS 보안 설정, 빌드 환경 복구 · 배포 절차 문서화
PHP	PHP 5 · 7 · 8.x, 자체 개발 · CMS 기반 시스템	PHP 8.4 업그레이드, 삭제 함수 · 라이브러리 수정
ASP · .NET	Classic ASP, ASP.NET WebForms · MVC (C#)	보안 조치, .NET 지원 버전 전환, IIS 설정 정비
Node.js · Python	Express · NestJS, Django · Flask 등	런타임 LTS 전환, 패키지 취약점 조치
프론트엔드 · 앱	jQuery · Vue · React, 하이브리드 앱	화면 보안 조치, 라이브러리 업데이트
최신 시스템	Spring Boot · NestJS · Next.js · React · Vue, 클라우드(AWS 등)	운영 · 보안 점검, 기능 개선, 장애 대응
DB · 서버	Oracle · MySQL · MariaDB · MS-SQL, CentOS · Ubuntu · Windows Server	DB 버전 업, 지원 종료 OS 이전, 서버 이관

취약 라이브러리(Log4j 1.x · 취약 버전 2.x, Struts, Commons FileUpload · Collections, 구버전 Jackson 등) 교체도 함께 진행합니다. 2026년 10월 공개된 PHP 원격 코드 실행 취약점에 대응해 운영 중인 고객 시스템의 PHP 버전 업그레이드를 순차 수행하고 있으며, 자바포셸(Java4Shell, CVE-2026-114938) 등 최신 보안 이슈의 점검 방법과 패치 순서는 보안 칼럼으로 안내하고 있습니다.

PROCESS

진행 절차 — 점검표 접수부터 매달 운영까지

점검 일정이 촉박해도 괜찮습니다. 점검표를 보내주시면 미흡 항목과 조치 일정부터 정리해 드립니다. 외주 재하청 없이 개발팀이 직접 수행하므로 의사결정과 개발이 빠릅니다.

01
점검표 접수
고객사 체크리스트와 점검 일정 확인

02
현황 진단
시스템 · 서버 · 계정 현황을 항목별로 대조

03
조치 계획
미흡 항목, 조치 방법, 우선순위, 일정 제안

04
조치 개발
인증 · 권한 · 암호화 · 로그 · 파기 기능 구현

05
증적 · 회신
항목별 증적 캡처, 회신서 작성 지원, 재점검 대응

06
월간 운영
접속기록 점검, 패치, 계정 정리, 장애 대응

레거시 시스템 인수 절차

자료 확인	소스, 운영 서버 접근 권한, 관리자 · 테스트 계정, 남아 있는 문서 확인
구조 · 버전 진단	언어 · 프레임워크 · WAS · 라이브러리 버전, 빌드 방식, DB 구조, 보안 취약점 정리
범위 · 견적 제안	유지보수 범위와 우선 조치할 보안 · 업그레이드 항목 제안
안정화	빌드 · 배포 환경 복구, 백업 체계 정비, 긴급 취약점 조치
월간 운영	장애 대응, 기능 개선, 월간 보안 점검, 단계적 버전 업그레이드

PRICING

무료 진단 후 견적

정확한 범위는 시스템 규모와 점검 항목 수에 따라 달라집니다.
무료 진단: 보안점검 체크리스트 검토 · 레거시 시스템 인수 진단 · PHP · 서버 버전 점검.
진단만 받고 끝내셔도 됩니다.

CASE STUDY

수행 사례 ① — 2년간 8차례의 보안점검, 이렇게 대응했습니다

잔존물 경매 시스템은 여러 고객사로부터 개인정보 처리를 위탁받아 매년 고객사별 보안점검을 받습니다. 점검하는 회사마다 양식도, 항목도, 요구하는 증적도 다릅니다.

8회
보안점검 · 이행점검 대응

200+
점검표 항목

22건
보안심사 지적 사항 조치

70건
증적 자료

STEP 1 · 200개가 넘는 항목

고객사마다 다른 점검표, 합치면 200개가 넘는 항목. 같은 내용도 묻는 방식이 달라 항목마다 현황을 다시 확인하고 답변을 새로 작성했습니다.

STEP 2 · 문서가 아니라 기능으로

1·2차 보안심사 지적 22건을 시스템 기능으로 구현: 로그인 문자 인증, 5회 실패 잠금, 장기 미접속 차단, 동시 접속 제한, DB · 첨부파일 암호화, 암호키 분리, 개인정보 파기 등.

STEP 3 · 증적과 회신서까지

점검 항목 번호에 맞춰 화면 · DB · 서버 설정 증적 70건을 캡처하고, 고객사 회신 양식에 맞춰 조치 내용을 정리했습니다.

2025
정기 점검 2회
금융사 위탁업체 정기 점검, 증적 자료 작성

2026.06
사전 질의 · 보안심사 2회
사전 환경 질의서 회신, 1·2차 심사 지적 22건 접수

2026.07~10
조치 기능 개발
인증 · 권한 · 암호화 · 로그 · 파기 기능 구현

2026.08
정기 점검 2회
추가 금융사 정기 점검 대응

2026.10
PHP 8.4 보안 업그레이드
원격 코드 실행 취약점 대응, 웹셸 · 테스트 파일 제거

2026.11
이행점검 2회
긴급점검 이행 회신(증적 70건), 보완 이행점검 대응

※ 고객사 보호를 위해 업체명과 자료 내용은 공개하지 않습니다.

PORTFOLIO

수행 사례 ② — 개발 · 유지보수해 온 시스템

대기업 · 금융 · 보험 · 공공기관부터 스타트업 플랫폼까지, 언어와 규모에 상관없이 개발하고 유지보수해 왔습니다. (고객사명은 홈페이지와 동일하게 일부 마스킹)

보안 운영
잔존물 경매 시스템
보안점검 대응 · 월간 접속기록 점검 · PHP 8.4

보안 운영
경매 플랫폼
경매 · 셀러 · 관리 시스템 · PHP 8.4

금융
현대xxx
캐피탈 · 카드 · 커머셜 퇴직 · 위반자 관리 시스템

보험
Axxx
VROBS 신용정보법 대응 시스템

기업 시스템
태산xxx
영업관리 · 레포팅 · 인사관리 시스템, DRM · VPN

HR
마인xxx
HR 진단 솔루션 · 레포팅 시스템

HR
랫xxx
HR 시스템

기업 시스템
알xxx
R프로젝트 · S프로젝트

공공
인천xxx
보호구역 방문증 Self 발급 소프트웨어

공공
서울시xxx
빅데이터 플랫폼 유지보수

공공
축산xxx
빅데이터 분석 시스템

빅데이터
빅데이터 수집 시스템
데이터 수집 · 적재 · 관리

AI
AI 주식 트레이딩 시스템
시세 분석 · 자동매매

플랫폼
이지xxx
헬스케어 플랫폼 개발 · 운영

플랫폼
탑xxx
홈페이지 · 서비스 운영

커머스
Wxxx
쇼핑몰 운영 · 유지보수

플랫폼
뉴젠xxx
NFT 거래 플랫폼

플랫폼
아우터xxx
배우웨이 플랫폼

솔루션
TrackSync
보안백업 솔루션 (자체 개발)

홈페이지
기업 · 기관 홈페이지
반응형 홈페이지 · 관리자 시스템 다수

운영 중인 Java 시스템 예시 태산xxx: Spring Boot 2.7 · 3.3, Java 17, JPA · QueryDSL, Spring Security | 마인xxx: Spring Boot 2.7, Java 17 | 이지xxx: Spring Boot 2.7, Java 11

WHY GENERIC IT

왜 제너릭아이티인가

레거시 유지보수 업체를 고를 때 확인해야 할 7가지, 제너릭아이티는 모두 직접 수행합니다.

01
다른 업체 시스템 인수 경험
매뉴얼 · 테스트 계정 · 소스 · 서버 현황을 분석해 이어받아 운영합니다.

02
레거시부터 최신 기술까지
PHP · Java(JSP · Spring) · ASP · .NET · Node.js · Python 등 언어와 상관없이 대응합니다.

03
지원 종료 버전 업그레이드
고객 시스템 PHP 8.4 보안 업그레이드 등 실제 업그레이드 경험을 바탕으로 깨지는 코드를 직접 수정합니다.

04
매달 보안 상태 보고
월간 접속기록 점검 보고서, 계정 정리, 보안 업데이트 확인 기록을 남깁니다.

05
고객사 보안점검 대응 경험
대형 금융사 보안점검 · 이행점검 8회, 200여 개 항목을 직접 대응했습니다.

06
재하청 없이 직접 수행
외주 재하청 없이 개발팀이 직접 수행하므로 의사결정과 개발이 빠릅니다.

07
고객 명의 자산 관리
소스 · 서버 · 계정을 고객 명의로 관리합니다.

기능으로 해결
지적 사항은 문서가 아니라 기능으로 해결합니다. 컨설팅 업체의 진단 보고서를 받은 뒤 조치 개발만 맡기셔도 됩니다.

CONTACT

고객사 보안점검, 오래된 시스템,
혼자 고민하지 마세요

점검표나 현재 상황만 알려주시면 미흡 항목과 조치 일정부터 정리해 드립니다.
비용은 **무료 진단 후 견적**으로 안내해 드립니다.

이메일	dh.kang@genericit.co.kr
전화	02-6338-6707
팩스	070-8668-0339
홈페이지	www.genericit.co.kr
주소	경기도 남양주시 다산순환로 20 현대프리미엄 캠퍼스 A동

(주)제너릭아이티 | 대표 강덕훈 | 사업자등록번호 238-86-02252
Copyright ⓒ Generic IT Corporation. All rights reserved.