KISEC

정보보안
특강 패키지 소개서

2025. 04.

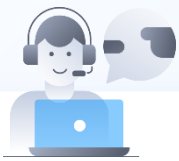
KISEC

정보보안 특강 패키지란?

"모든 보안사고의 시작은 사람에서 비롯됩니다."

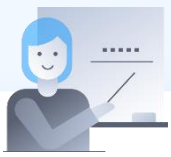
정보보안 특강 패키지는 기업의 보안 수준 향상을 위한 맞춤형 보안 교육 패키지입니다.
전 직원이 수강이 가능한 쉬운 난이도의 특강부터 IT직군만을 위한 교육과정, 그리고 악성메일에 대비하기 위한 과정까지 직무별, 상황별 보안 역량 강화를 위한 커리큘럼이 다양하게 구성되어 있습니다. 직원들의 특성을 고려한 특강을 통해, 임직원의 보안 인식 변화를 유도하여 기업에서의 실천하는 보안 문화를 정착시킬 수 있도록 합니다.

특강 수강 방법



온라인 실시간

강사와 온라인
실시간으로 서로 쌍방
소통하며 교육을
수강합니다.



오프라인

강사와 함께 현장감
있는 교육을 통해
효과를 극대화 합니다.

On-Demand

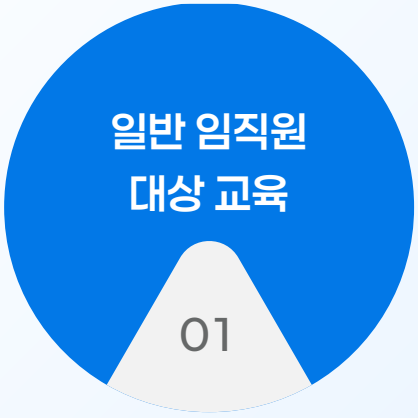
시공간 제약 없이
언제든지 수강이
가능한 환경을
제공합니다.

특강 과정 선택 방법

교육문의 | KISEC 교육사업부 02-921-1465 edu@kisec.com

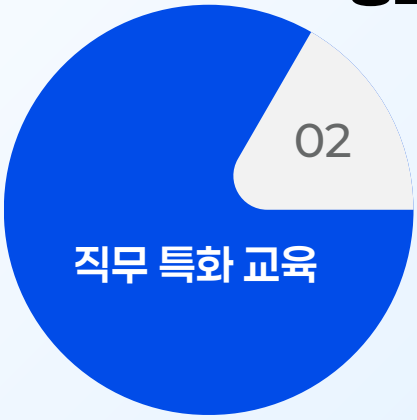
KISEC

3가지 테마로 이루어진 정보보안 특강 패키지를 소개합니다!



IT·정보보안 전공이 아니어도 좋아요. 우리 회사의 보안 수준이 강화될 수만 있다면!

우리회사 보안 수준 강화를 위한 정보보안 특강 패키지!

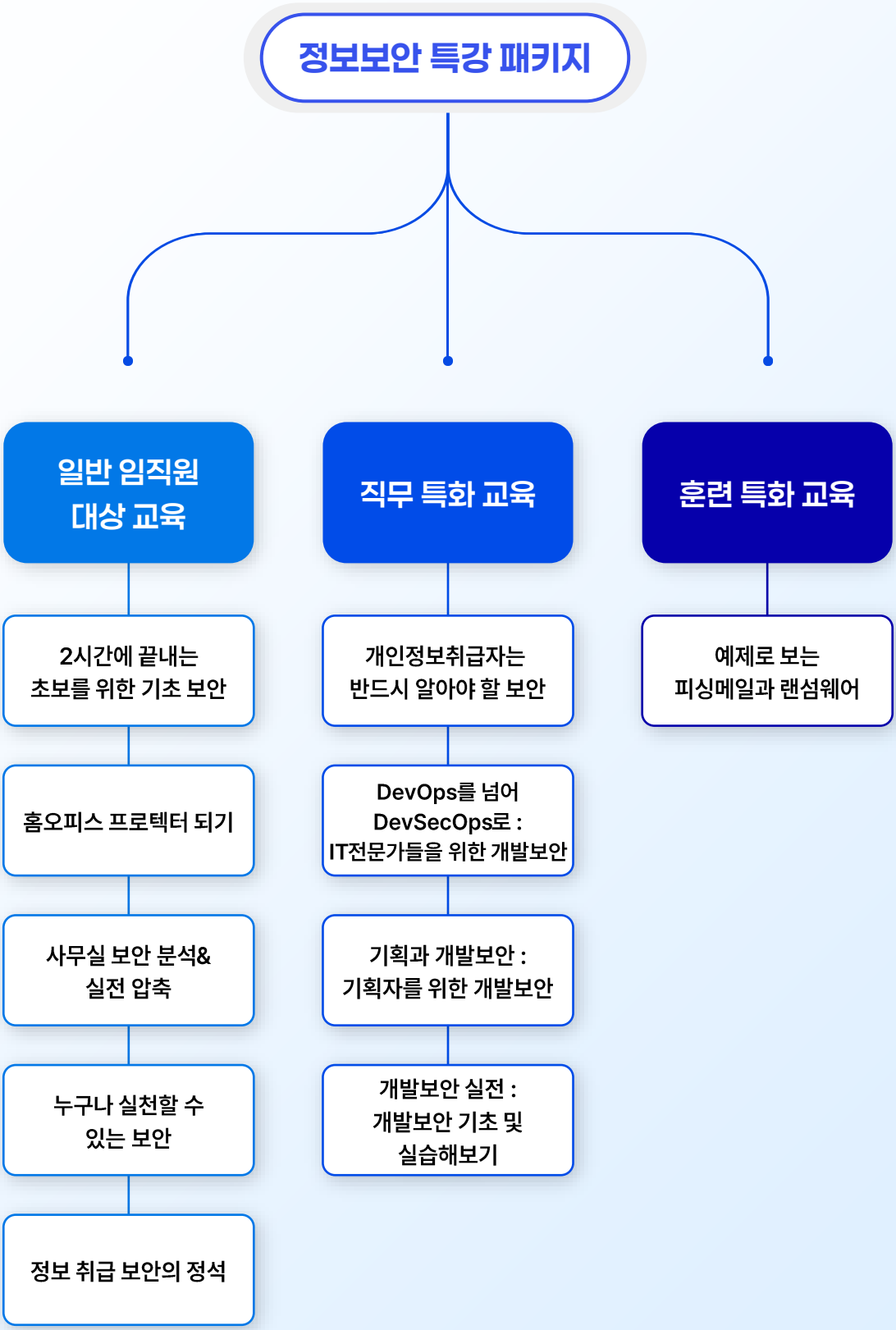


전공자들이 시시하지도, 뻔하지도 않을 조금 수준 있는 교육을 받고 싶어요!

악성메일훈련, 사고대응 모의 훈련 등 기업 훈련 이후 경각심을 한번 더! 일깨우기 위한 교육이에요.

KISEC

정보보안 추천 과정



KISEC

01. 일반 임직원 대상 교육

"일반 임직원 대상 교육"에서는 IT 또는 정보보안 비전공 직무에서도 이해하기 쉬운 내용들로 구성되어 있으며, 다양한 사례를 기반으로 우리 회사 임직원의 보안 수준 강화를 위한 교육 패키지 구성이 되어 있습니다.

일반 임직원 대상 교육

- 하나만 듣는게 아닌 보편적인 내용으로 듣고 싶다면
- 재택근무 시 보안을 지키는 방법을 알고 싶어요
- 내가 근무하는 사무실에서 보안을 어떻게 하죠?
- 입사하는 신입직원들도 들을 수 있는 쉬운 보안 교육 있을까요?
- 고객정보를 보호하는 방법을 알고 싶다면

과정추천

기초보안

2시간에 끝내는 초보를 위한 기초 보안

신입 보안 교육 | 하 | 2h

오피스보안

사무실 보안 분석 & 실전 압축

사무실 보안 | 하 | 1h

정보취급 보안교육

정보 취급 보안의 정석

개인정보 & 영업비밀 보안 | 하 | 1.5h

재택근무

홈오피스 프로텍터 되기

재택근무자 대상 | 하 | 2h

다방면 보안 역량 강화

누구나 실천할 수 있는 보안

일반 보안 교육 | 하 | 2h

02. 직무 특화 교육

"직무 특화 교육"은 IT 또는 정보보안 직무에서 실무에서 필요한 보안지식을 학습하고 업무에서 활용할 수 있도록 구성되어 있습니다. 실무 적용을 위한 구체적인 가이드 및 예시와 함께 실습을 겸하는 과정이 준비되어 있습니다.

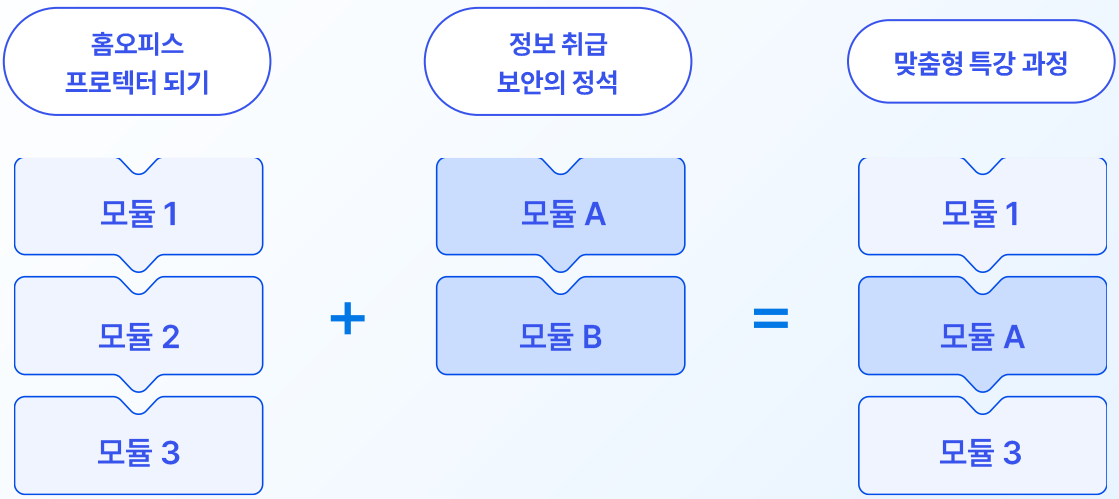
03. 훈련 특화 교육

"훈련 특화 교육"에서는 사전에 악성메일 훈련이나 침해사고 대응 훈련(모의훈련) 이후 경각심과 대처 방안을 다시한번 일깨워줄 수 있도록 효과를 극대화 합니다. 기업 내 여러 훈련이 필요하다면 언제든 문의 바랍니다.

KISEC

그 밖에 우리 회사에 맞는 특강을 원한다면?

CASE 01 세분화된 각 모듈 선택이 가능해요!



추천 과정 외에도 세분화된 과정 모듈에서 필요한 모듈을 선택해 우리 회사에 필요한 내용으로 구성할 수 있어요.

CASE 02 우리 회사에 특화된 교육을 원합니다.

커스터마이징 교육 개발 절차

고객사 요구사항 협의 (강의 형태 선택)	교육 설계	교안 제작	강사 섭외	교육 또는 영상 시청	수료 결과 보고
수강형식 및 커리큘럼 선택, 특강 요구사항 수렴	특강 요구사항에 맞춘 커리큘럼 커스터마이징	커스터마이징한 커리큘럼에 맞춰 교안 제작	전문 강사 배정	협의한 일정, 장소, 방법에 따라 교육 수강	수강 현황 및 수료 결과 보고, 필요 시 수료증 발급

기업 특성에 맞는 교육 설계 및 개발이 필요하다면 담당자에게 문의 바랍니다.

정보보안 특강패키지

추천 과정을 소개합니다!

KISEC

01 2시간에 끝내는 초보를 위한 기초 보안

신입 보안 교육

추천 대상

회사 내 보안 준수 사항을 잘 모르는 신규 입사자

회사 내 보안 지식이 얕은 직원

정보보안과 관련한 기초 소양이 부족한 직원

과정 목표

1. 실제 보안 사건/사고 사례를 통해 정보보안의 중요성을 체감하고 기본 개념을 이해한다.
2. 업무자료 보안 및 정보보호 기본 수칙을 일상 업무에 자연스럽게 적용할 수 있는 습관을 형성한다.
3. 보안 위협에 직면했을 때 적절하게 대응하고 보고할 수 있는 절차와 방법을 숙지한다.

→ 정보보안 인식 향상

→ 정보보호 생활화

→ 보안 사고 대응력 강화

교육 내용

정보보안 사고 및 개인정보유출 사고 사례 및 정보보호와 개인정보보호의 정의에 대하여 학습

피싱메일, USB등의 매체를 통한 공격기법과 대응법 소개

업무자료 등의 업무 환경에서 수행할 수 있는 보안활동 소개 및 정보보호를 위한 수칙 소개

KISEC

01 2시간에 끝내는 초보를 위한 기초 보안

신입 보안 교육 | 난이도 | 하 | 총 2시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
정보보호의 필요성	• 정보보안 사건/사고 사례 • 정보보호 기본 개념의 이해 • 정보보호의 의미	이론 / 사례	30
개인정보보호란?	• 개인정보 유출 사고 사례 • 개인정보의 유형과 종류 • 개인정보보호의 목적 • 개인정보보호의 정의	이론 / 사례	30
USB를 주의해야하는 이유	• USB 보안과 USB를 활용한 공격	이론	15
예시로 알아보는 피싱메일 수법	• 피싱 메일의 유형과 특징 • 피싱 메일 공격 예방 및 대응 방법	이론 / 사례	15
보안을 좀 아는 우리 직원들	• 흔한 사무실 풍경 속 다양한 보안 빈틈 찾아내기 • 개성 있는 화면보호기와 비밀번호 설정 • 업무자료 보안 방법 • 임직원 정보보호 기본 수칙	이론	30

KISEC

02 홈오피스 프로텍터 되기

재택근무자 대상

추천 대상

원격근무 또는
재택근무를
처음 시작하는 임직원

원격근무 또는
재택근무 중에 보안 사고
경험이 있는 임직원

원격 근무 시 어떤
위험 사항이 있는지
궁금한 직원

과정 목표

1. 재택근무 환경에서 발생하는 특수한 보안 위협과 사례를 이해하고, 정보보호의 중요성을 재인식한다.
   → 원격 근무 보안 인식 제고

2. 가정 및 외부 네트워크 환경에서 발생할 수 있는 보안 취약점을 인지하고, 이에 적절히 대응할 수 있는 능력을 배양한다.
   → 원격 보안 위협 대응 능력 강화

3. 다양한 원격 근무 형태에 따른 맞춤형 정보보안 수칙을 이해하고 일상적으로 실천할 수 있는 습관을 형성한다.
   → 원격 근무 보안 수칙 실천

교육 내용

정보보안 사고 및 개인정보유출 사고 사례 및 피싱메일, USB등의
원격 근무에서 발생할 수 있는 매체 기반 공격과 대응법 소개

원격 근무의 정의, 원격 근무 환경의 특성과 이를 기반으로 한
사고 사례 및 원격 근무 실천 수칙 소개

정보보호를 위한 수칙에 대하여 학습

KISEC

02 홈오피스 프로텍터 되기

재택근무자 대상 | 난이도 | 하 | 총 2시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
정보보호의 필요성	• 정보보안 사건/사고 사례 • 정보보호 기본 개념의 이해 • 정보보호의 의미	이론 / 사례	30
예시로 알아보는 피싱메일 수법	• 피싱 메일의 유형과 특징 • 피싱 메일 공격 예방 및 대응 방법	이론 / 사례	30
원격 근무에서도 존재하는 위험	• 원격 근무 환경 위협 이해 • 원격 근무 정보보안 수칙	이론 / 사례	45
정보보호 기본 수칙	• 임직원 정보보호 기본 수칙	이론	15

KISEC

03 사무실 보안 분석 & 실전 압축

사무실 보안

추천 대상

사회 공학적 해킹을
모르는 임직원

안전한 사무실 환경을
유지하고 싶은 직원

사무실 환경 관리 미흡으로
사고를 경험하거나
피해를 입었던 직원

과정 목표

1. 다양한 사회공학 기법의 유형과 특징을 이해하고, 이를 식별하여 적절히 대응할 수 있는 능력을 배양한다.
   → 사회공학적 공격 인식 능력 향상

2. USB 저장장치를 통한 보안 위협을 인지하고, 안전한 USB 사용법과 관리 방법을 습득한다
   → USB 보안 관리 역량 강화

3. 업무자료의 관리 방법과 정보보호 기본 수칙을 일상 업무에 자연스럽게 적용할 수 있는 습관을 형성한다.
   → 정보자산 보호 습관화

교육 내용

시청각 자료를 통한 사회공학 기법의 정의 및 유형 학습

USB 등의 매체를 통한 공격 기법과 대응법 소개

업무자료 등의 업무 환경에서 수행할 수 있는 보안활동 소개 및 정보보호를 위한 수칙 소개

KISEC

03 사무실 보안 분석 & 실전 압축

사무실 보안 | 난이도 | 하 | 총 1시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
신뢰를 악용하는 그들의 기법	• 사회공학 기법	이론 / 사례	15
USB를 주의해야하는 이유	• USB 보안과 USB를 활용한 공격	이론	15
보안을 좀 아는 우리 직원들	• 흔한 사무실 풍경 속 다양한 보안 빈틈 찾아내기 • 개성 있는 화면보호기와 비밀번호 설정 • 업무자료 보안 방법 • 임직원 정보보호 기본 수칙	이론	30

KISEC

04 누구나 실천할 수 있는 보안

일반 보안 교육

추천 대상

사이버 정보보안이 궁금한 임직원

피싱메일이나 랜섬웨어 대처법이 궁금한 임직원

개인정보보호 활동에 대해 궁금한 임직원

과정 목표

1. 피싱 메일과 랜섬웨어의 특징을 파악하고, 효과적인 예방 및 대응 방법을 습득하여 실제 상황에서 적용할 수 있는 능력을 기른다.

→ 사이버 위협 대응 능력 강화

2. 사무실 환경에서의 보안 취약점을 스스로 식별하고 개선할 수 있는 판단력과 실행력을 함양한다.

→ 보안 취약점 식별 및 개선 능력 배양

3. 효과적인 비밀번호 관리, 화면보호기 설정, 업무자료 보안 관리 등 기본적인 정보보호 수칙을 일상 업무에 적용하는 습관을 형성한다.

→ 정보 자산 보호 실천

교육 내용

정보보안 사고 및 개인정보유출 사고 사례 및 정보보호와 개인정보보호의 정의에 대하여 학습

피싱메일, USB 등의 매체로 인한 보안 위협, 랜섬웨어의 특징 및 예방·대응법 소개

업무자료 등의 업무 환경에서 수행할 수 있는 보안활동 소개 및 정보보호를 위한 수칙 제시

KISEC

04 누구나 실천할 수 있는 보안

일반 보안 교육 | 난이도 | 하 | 총 2시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
정보보호의 필요성	• 정보보안 사건/사고 사례 • 정보보호 기본 개념의 이해 • 정보보호의 의미	이론 / 사례	30
예시로 알아보는 피싱메일 수법	• 피싱 메일의 유형과 특징 • 피싱 메일 공격 예방 및 대응 방법	이론 / 사례	15
랜섬웨어 파헤치기	• 랜섬웨어 • 랜섬웨어 예방법과 대응방법	이론 / 사례	15
사례로 보는 개인정보 유출의 위험성	• 개인정보 유출 사고 사례 • 개인정보보호의 목적 • 개인정보보호의 정의 • 개인정보 관련 인식 변화 • 개인정보 노출 원인별 사례 • 개인정보보호 원칙	이론 / 사례	30
보안을 좀 아는 우리 직원들	• 흔한 사무실 풍경 속 다양한 보안 빈틈 찾아내기 • 개성 있는 화면보호기와 비밀번호 설정 • 업무자료 보안 방법 • 임직원 정보보호 기본 수칙	이론	30

KISEC

05 정보 취급 보안의 정석

개인정보 & 영업비밀 보안

추천 대상

개인정보보호 활동에 대해 궁금한 임직원

영업비밀의 활동 범위와 기준이 궁금한 직원

개인정보보호와 영업비밀 활동의 차이가 궁금한 임직원

과정 목표

1. 개인정보보호의 기본 원칙을 이해하고 일상 업무에 적용할 수 있는 실천력을 배양한다.
2. 영업비밀의 정의와 유출 시 발생하는 구체적인 피해를 이해함으로써 영업비밀 보호의 필요성을 인식한다.
3. 영업비밀 사건의 다양한 측면을 이해하고, 실제 유출 사례 분석을 통해 영업비밀 보호를 위한 실질적인 방법을 습득한다.

개인정보보호 원칙 적용 | 영업비밀 중요성 인식 | 영업비밀 보호 역량 강화

교육 내용

개인정보의 정의와 유형·분류, 개인정보유출 사고 사례, 개인정보 유·노출 유형별 발생 원인 및 대처방법 학습

영업비밀의 정의, 성립요건과 영업비밀 유출 사례, 유출 시 발생하는 피해 학습

정보보호를 위한 기본 수칙 학습

KISEC

05 정보 취급 보안의 정석

개인정보 & 영업비밀 보안 | 난이도 | 하 | 총 1.5시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
사례로 보는 개인정보 유출의 위험성	• 개인정보 유출 사고 사례 • 개인정보보호의 목적 • 개인정보보호의 정의 • 개인정보 관련 인식 변화 • 개인정보 노출 원인별 사례 • 개인정보보호 원칙	이론 / 사례	30
영업비밀보호	• 영업비밀보호의 정의 • 영업비밀 유출 시 피해 • 영업비밀 사건의 두 측면 • 영업비밀 유출 사례 • 검·경·청 강화하는 영업비밀 관련 보호활동	이론	30
보안을 좀 아는 우리 직원들	• 흔한 사무실 풍경 속 다양한 보안 빈틈 찾아내기 • 개성 있는 화면보호기와 비밀번호 설정 • 업무자료 보안 방법 • 임직원 정보보호 기본 수칙	이론	30

KISEC

06 개인정보취급자는 반드시 알아야 할 보안

정보취급자 대상

추천 대상

개인정보처리자 & 개인정보취급자 직무를 수행중인 임직원

개인정보관련 업무를 담당 OR 담당 예정인 임직원

개인정보보호와 관련된 업무를 수행해야 하는 직원

과정 목표

1. 실제 개인정보 유출 사고 사례와 이로 인한 과징금, 과태료 부과 사례를 분석하여 개인정보 관리의 중요성과 책임성을 인식한다.
   → 개인정보보호 현황 인식
2. 개인정보보호법의 핵심을 이해하여 법적 요구사항에 부합하는 개인정보 관리 체계를 구축할 수 있는 지식을 습득한다.
   → 법률적 지식 함양
3. 개인정보보호 8대 원칙을 심층적으로 이해하고, 이를 실무에 적용할 수 있는 구체적인 방법론을 습득한다.
   → 개인정보보호 원칙 실천

교육 내용

개인정보의 정의와 유형·분류 및 개인정보에 대한 인식변화에 대한 내용,
개인정보유출 사고와 사고 발생시 과징금 부과 사례 등을 수록

개인정보보호법을 쉽게 이해할 수 있도록 법 용어와 핵심포인트를 살펴보고
개인정보보호법의 핵심 조항을 학습

개인정보 유·노출 사고 발생시 취해야하는 후속 조치, 안정성 확보를 위한 조치사항들,
정보보호를 위한 수칙 숙지

KISEC

06 개인정보취급자는 반드시 알아야 할 보안

정보취급자 대상 | 난이도 | 중 | 총 2시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
사례로 보는 개인정보 유출의 위험성	• 개인정보 유출 사고 사례 • 개인정보의 유형과 종류 • 개인정보보호의 목적 • 개인정보보호의 정의 • 개인정보 노출 원인별 사례 • 개인정보 유출로 인한 과징금, 과태 부과 사례 • 개인정보 관련 인식 변화 • 개인정보보호 원칙	이론 / 사례	30
개인정보보호법 알아보기	• 개인정보보호법 관련 용어 • 개인정보보호법 핵심 포인트 • 개인정보보호 8대 원칙 • 개인정보보호법 중요 조항	이론	60
개인정보보호 수칙	• 개인정보의 유출 및 노출 시 조치사항 • 운영자가 특히 알아야 하는 예방수칙 • 임직원 정보보호 기본 수칙	이론	30

KISEC

07 DevOps를 넘어 DevSecOps로 : IT전문가들을 위한 개발보안

개발보안 통합

추천 대상

IT·인프라 직무에
종사 중인 임직원

개발 프로젝트에서
보안을 적용하고자 하는
기획자 및 개발자

개발보안 적용 예정인
프로젝트에 참여 OR
참여할 예정인
기획자 및 개발자

과정 목표

1. 최신 SW개발보안 사고 사례, 핵심 키워드, OT/IT 사건/사고 사례 분석을 통해 개발보안의 중요성과 위협 환경을 이해한다.
   → 개발보안 환경 인식 제고
2. 개발보안 방법론의 단계별 개발보안 활동을 습득하여 전체 개발 과정에서의 보안 통합 능력을 강화한다.
   → 개발 생명주기별 보안 활동 숙지
3. 실습을 통해 시큐어 코딩 기법을 직접 적용해보고, 코드 레벨에서의 보안 취약점을 식별하고 개선할 수 있는 실질적인 능력을 기른다.
   → 시큐어 코딩 실무 능력 배양

교육 내용

IT 동향 및 여러 산업군에서의 개발보안 사고사례, 국내외 개발보안 정책·제도의 흐름, 개발보안 도입 시의 이점과 실 개발보안 도입 사례 소개

개발보안의 정의 및 개발보안 방법론 및 SW개발 프로젝트에서의 직무별·단계별 수행가능한 보안활동들 소개

프로그래밍 언어별 시큐어 코딩 예제에 대한 실습 포함

KISEC

07 DevOps를 넘어 DevSecOps로 : IT전문가들을 위한 개발보안

개발보안 통합 | 난이도 | 상 | 총 4시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
SW개발보안 왜 필요할까	• 최신 SW개발보안 사고 핵심 키워드 • 개발보안 사건/사고 사례 • OT 사건/사고 사례 • IT 기술 트렌드 • 개발보안 동향	이론 / 사례	30
SW개발보안 알아보기	• 소프트웨어 개발보안 정의 • 보안약점과 취약점 비교 • CVE와 CWE • 소프트웨어 개발보안 적용 사례 • SW개발보안 기대효과 • SW개발보안 가이드	이론 / 사례	90
개발보안 방법론과 단계별 보안활동	• 개발보안 방법론 • 소프트웨어 개발보안 방법론 • 개발 프로젝트 직무별 개발보안 • 분석 단계 개발보안 활동 • 설계 단계 개발보안 활동	이론 / 사례	60
시큐어 코딩 맛보기	• 시큐어 코딩 실습	이론	60

KISEC

08 기획과 개발보안 : 기획자를 위한 개발보안

기획자 특화

추천 대상

개발 프로젝트에서 보안을 적용하고자하는 기획자 및 운영자

개발보안을 적용 중인 프로젝트에 참여 예정인 기획자 및 운영자

프로젝트 수행 단계별로 개발보안 적용이 필요한 기획 및 운영 담당 직원

과정 목표

1. 프로젝트 특성에 맞는 효과적인 보안 계획을 수립하고, 설계 단계에 적용하는 방법론을 이해한다.
   → 보안 계획 수립 능력 개발
2. 주요 보안설계 기준의 정의와 고려사항을 이해하고, 설계 명세에 반영할 수 있는 능력을 배양한다.
   → 보안설계 기준 적용 역량 습득
3. 보안 요구사항과 설계 기준을 개발팀에 명확히 전달하고 협업할 수 있는 의사소통 능력을 향상시킨다.
   → 개발팀과의 소통 역량 강화

교육 내용

IT 동향 및 여러 산업군에서의 개발보안 사고사례 및 국내외 개발보안 정책·제도의 흐름, 개발보안 도입 시의 이점과 실 개발보안 도입 사례 소개

개발보안과 개발보안 방법론의 정의 학습

SW개발 프로젝트에서의 단계별 수행 가능한 보안활동들과 관련 산출물 예제 제시

KISEC

08 기획과 개발보안 : 기획자를 위한 개발보안

기획자 특화 | 난이도 | 상 | 총 3시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
SW개발보안 왜 필요할까	• 최신 SW개발보안 사고 핵심 키워드 • 개발보안 사건/사고 사례 • OT 사건/사고 사례 • IT 기술 트렌드 • 개발보안 동향 • 사고사례 파악하기	이론 / 사례	30
SW개발보안과 방법론	• 소프트웨어 개발보안 정의 • 보안약점과 취약점 비교 • 개발보안 방법론 • 소프트웨어 개발보안 방법론	이론 / 사례	30
개발보안 방법론과 단계별 보안활동	• 개발보안 방법론 • 소프트웨어 개발보안 방법론 • 개발 프로젝트 직무별 개발보안 • 분석 단계 개발보안 활동 • 설계 단계 개발보안 활동	이론 / 사례	120

KISEC

09 개발보안 실전 : 개발보안 기초 및 실습해보기

개발자 특화

추천 대상

개발보안 적용 예정인 프로젝트에 참여 중인 개발자

개발보안이 적용된 프로젝트에 새롭게 참여하는 개발자

개발보안이 무엇인지 이론 뿐 아니라 실습으로도 체험해보고 싶은 개발자

과정 목표

1. 최신 SW개발보안 사고 사례와 핵심 키워드 분석, IT/OT 영역의 실제 사건/사고 사례를 통해 현재의 위협 환경을 이해한다.

→ 개발보안 환경 이해

2. 소프트웨어 개발보안의 정의와 보안약점·취약점의 차이점을 명확히 이해하고, SW개발보안의 기대효과를 인식한다.

→ 개발보안 개념 심화

3. 다양한 프로그래밍 언어와 개발 환경에서의 시큐어코딩 실습을 통해 코드 레벨에서 보안 취약점 식별 및 제거하는 기술을 습득한다.

→ 시큐어코딩 실무 역량 강화

교육 내용

IT 동향 및 여러 산업군에서의 개발보안 사고사례, 국내외 개발보안 정책·제도의 흐름, 개발보안 도입 시의 이점과 실 개발보안 도입 사례 제시

개발보안의 정의와 보안약점과 취약점의 차이, 개발보안 가이드 의 종류와 특징 소개

프로그래밍 언어별 시큐어 코딩 예제에 대한 실습 포함

KISEC

09 개발보안 실전 : 개발보안 기초 및 실습해보기

개발자 특화 | 난이도 | 상 | 총 3시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
SW개발보안 왜 필요할까	• 최신 SW개발보안 사고 핵심 키워드 • 개발보안 사건/사고 사례 • OT 사건/사고 사례 • IT 기술 트렌드 • 개발보안 동향 • 사고사례 파악하기	이론 / 사례	30
SW개발보안 알아보기	• 소프트웨어 개발보안 정의 • 보안약점과 취약점 비교 • CVE와 CWE • 소프트웨어 개발보안 적용 사례 • SW개발보안 기대효과 • SW개발보안 가이드	이론 / 사례	90
시큐어 코딩 맛보기	• 시큐어 코딩 실습	이론	60

KISEC

10 예제로 보는 피싱메일과 랜섬웨어

피싱 메일 특화

추천 대상

기업 내에서 악성메일이나 랜섬웨어 훈련을 받을 예정인 임직원

피싱메일과 랜섬웨어의 예방·대응 방안을 알고 싶은 임직원

피싱메일 또는 랜섬웨어 사고를 경험하거나 피해를 입었던 직원

과정 목표

1. 정상 메일과 피싱 메일을 구분할 수 있는 판별력과 피싱 메일에 대한 예방 및 대응 절차를 숙지하고, 실제 상황에서 능력을 배양한다.

→ 피싱메일 식별 능력+ 피싱대응 프로세스 습득

2. 랜섬웨어 감염 예방법과 감염 시 대응 방법을 습득하여 피해를 최소화할 수 있는 기술적·관리적 역량을 기른다.

→ 랜섬웨어 방어 역량 개발

3. 임직원 정보보호 기본 수칙을 일상 업무에 자연스럽게 적용하는 습관을 형성하여, 조직 내 보안 문화를 강화한다.

→ 보안 문화 내재화

교육 내용

국내외 사이버 공격 동향과 정보보안사고 사례 수록

피싱메일, 랜섬웨어의 특징과 이를 바탕으로 한 예방·대응법 소개

업무자료 등의 업무 환경에서 수행할 수 있는 보안활동 소개 및 정보보호를 위한 수칙 제시

KISEC

10 예제로 보는 피싱메일과 랜섬웨어

피싱 메일 특화 | 난이도 | 하 | 총 2시간 소요

과정 세부

대단원	중단원	교수법	단원별 소요시간(분)
사고사례로 보는 정보보안의 중요성	• 정보보안 사건/사고 사례	이론 / 사례	30
예시로 알아보는 피싱메일 수법	• 피싱 메일의 유형과 특징 • 피싱 메일 공격 예방 및 대응 방법	이론 / 사례	30
랜섬웨어 파헤치기	• 랜섬웨어 • 랜섬웨어 예방법과 대응방법	이론	30
정보보호 기본 수칙	• 임직원 정보보호 기본 수칙	이론	30