

I. 개 요

1. 직 종 명 : 보안엔지니어링

2. 직종 정의 : 보안엔지니어링은 정보 서비스의 보안 요구사항에 따라 정보보안시스템 도입을 위한 설계, 구축, 유지보수를 수행하는 업무에 종사.

3. 훈련이수체계(수준별 이수 과정/과목)

8	임원	SW아키텍처 이해 수립			
7	부장/차장	SW아키텍처 수행 관리 SW아키텍처요구사항 명세화 후보 SW아키텍처 탐색 SW아키텍처 설계 SW아키텍처 문서화	애플리케이션 요구사항 분석		개념데이터 모델링
6	과장/대리	SW아키텍처 요소기술연계 SW아키텍처 테스트 SW아키텍처 변경 관리	애플리케이션 리팩토링 인터페이스 설계 기능 모델링 애플리케이션 설계 정적모델 설계 동적모델 설계 소프트웨어공학 활용 소프트웨어개발 방법론 활용	운영체제 지식 데이터베이스 드라이버 분석 데이터베이스 드라이버 설계 데이터베이스 드라이버 구현 임베디드 SW 요구사항 분석	데이터베이스 요구사항 분석 논리 데이터베이스 설계 물리 데이터베이스 설계 데이터 품질관리 데이터베이스 성능측정 데이터전문 설계
5	사원	SW 개발 계획	요구사항 확인 데이터 입출력 구현 동작 구현 정보시스템 이행 개발소프트웨어 평가 서버프로그래밍 구현 인터페이스 구현 화면 설계 애플리케이션 테스트 관리	임베디드 시스템 테스트 필터 분석 필터 설계 필터 구현 운영체제 파일 분석 데이터베이스 드라이버 구현 환경 구축 임베디드 애플리케이션 분석 임베디드 애플리케이션 설계 임베디드 애플리케이션 구현	데이터 표준화 데이터관리 SQL응용
4	사원	SW아키텍처 이행		최드웨어 분석 기술문서 개발 필터 구현 환경 구축 임베디드 애플리케이션 구현 환경 구축	데이터베이스 구현
3	사원		애플리케이션 배포 프로그래밍 언어 활용 응용 SW 기초 기술 활용 화면 구현 애플리케이션 테스트 수행	오른 플랫폼 활용	SQL활용
-		직업기초능력			
수준	직종	SW아키텍처	응용SW엔지니어링	임베디드SW엔지니어링	DB엔지니어링

7	부장/차장	<div>네트워크 환경 분석</div> <div>네트워크 도중도서 설계</div> <div>네트워크 자원관리 설계</div> <div>네트워크 QoS 제어 설계</div> <div>네트워크 품질 평가</div> <div>네트워크 프로세스 관리</div> <div>네트워크 프로토콜 분석</div> <div>네트워크 프로토콜 설계</div>		<div>UI/UX 계획 수립</div>	<div>시스템SW 요구사항 분석</div> <div>시스템SW 아키텍처 설계</div>
6	과장/대리	<div>네트워크 소프트웨어 아키텍처 수립</div>	<div>관리직 보안 구축</div> <div>보안인증 관리</div>	<div>UI/UX 환경 분석</div> <div>사용자 리서치</div>	<div>시스템SW 상세 설계</div> <div>시스템SW 테스트</div> <div>시스템SW 기술문서 작성</div>
5	사원	<div>네트워크 소프트웨어 개발 방법 수립</div>	<div>보안 구축 계획 수립</div> <div>보안 구축 요구사항 분석</div> <div>소프트웨어 개발 보안 구축</div> <div>데이터베이스 보안 구축</div> <div>시스템 보안 구축</div> <div>네트워크 보안 구축</div>	<div>UI/UX 요구 분석</div> <div>UI/UX 콘셉트 기획</div> <div>UI 아키텍처 설계</div>	<div>시스템SW 통합 구현</div> <div>시스템SW 배포</div> <div>시스템SW 단위 모듈구현</div> <div>시스템SW 인터페이스 구현</div>
4	사원			<div>UI 디자인</div> <div>UI/UX 가이드 제작</div>	
3	사원	<div>네트워크 프로그램 개발 구현</div>	<div>관리직 보안 구축</div>	<div>UI 구현</div>	
2				<div>UI 테스트</div>	
-		직업기초능력			
수준	직종	NW엔지니어링	보안엔지니어링	UI/UX엔지니어링	시스템SW엔지니어링

<div>5과정/대리</div>		<div>핀테크 요구사항 분석</div>			
<div>5사원</div>		<div>핀테크 인프라 설계</div> <div>핀테크 인터페이스 설계</div> <div>핀테크 기능 설계</div> <div>핀테크 보안·인증 설계</div>			
<div>4사원</div>		<div>핀테크 인터페이스 구현</div> <div>핀테크 기능 구현</div> <div>핀테크 보안·인증 구현</div>			
<div>3사원</div>		<div>핀테크 테스트</div>			
-		직업기초능력			
수준	직종				
		빅데이터플랫폼구축	핀테크엔지니어링		

※ 해당직종(음영)의 훈련과정을 편성하는 경우 훈련과정별 목표에 부합한 수준으로 해당 직종에서 제시한 능력단위를 기준으로 과정/과목을 편성하고, 이외 직종의 능력단위를 훈련과정에 추가 편성하려는 경우 유사 직종의 동일 수준의 능력단위를 추가할 수 있음

4. 훈련시설

시설명 \ 훈련인원	기준인원	면 적	기준인원 초과 시 면적 적용	시설활용구분 (공용/전용)
강의실	20	45㎡	1명당 1.5㎡씩 추가	공용
컴퓨터실	20	45㎡	1명당 1.5㎡씩 추가	공용

※ 훈련시설은 훈련과정/과목에 필요한 시설을 구축

5. 교사

○ 「근로자직업능력 개발법」 제33조와 관련 규정에 따름

II. 훈련과정

○ 과정/과목명 : 직업기초능력

- 훈련개요

훈련목표	직업인으로서 갖추어야할 기본적인 소양을 함양
수 준	-
훈련시간	훈련과정 전체 교육시간의 10% 이내에서 자율편성
훈련가능시설	강의실 또는 컴퓨터실
권장훈련방법	집체훈련 또는 원격훈련

- 편성내용

단 원 명	학 습 내 용
의사소통능력	문서이해능력, 문서작성능력, 경청능력, 의사표현능력, 기초외국어능력
수리능력	기초연산능력, 기초통계능력, 도표분석 능력, 도표작성능력
문제해결능력	사고력, 문제처리능력
자기개발능력	자아인식능력, 자기관리능력, 경력개발 능력
자원관리능력	시간자원관리능력, 예산자원관리능력, 물적자원관리능력, 인적자원관리능력
대인관계능력	팀웍능력, 리더십능력, 갈등관리능력, 협상능력, 고객서비스능력
정보능력	컴퓨터활용능력, 정보처리능력
기술능력	기술이해능력, 기술선택능력, 기술적용능력
조직이해능력	국제감각, 조직체제이해능력, 경영이해능력, 업무이해능력
직업윤리	근로윤리, 공동체 윤리

○ 과정/과목명 : 2001020601_18v4 보안 구축 계획 수립

- 훈련개요

훈련목표	보안 구축 계획 수립이란 요구사항 분석 결과를 바탕으로 보안 환경을 분석하여 보안 범위를 설정하고, 보안 시스템 구축 계획을 수립하는 능력을 함양.
수 준	5수준
훈련시간	30시간
훈련가능시설	컴퓨터실
권장훈련방법	원격훈련, 집체훈련 실습

- 편성내용

단 원 명 (능력단위 요소명)	훈 련 내 용 (수행준거)
보안 범위 설정하기	1.1 보안 요구사항을 수집하여 보안 기능을 분류하고 분석할 수 있다. 1.2 분석된 보안 기능에 따라 필요한 인적·물적 자원을 나열할 수 있다. 1.3 나열된 자료를 통해 구축의 범위를 설정하고 일정 계획을 수립할 수 있다.
보안 아키텍처 설계하기	2.1 설정된 보안 범위에 따라 도출된 기능을 보안의 통제요소로 세분화할 수 있다. 2.2 세분화된 통제요소의 적용위치를 결정하고 상호관계를 분석할 수 있다. 2.3 보안 통제요소들을 충족하기 위해 기능간의 상호 관계를 설계할 수 있다. 2.4 설계 내역을 바탕으로 요구사항의 충족 여부를 확인하기 위하여 기능간의 상호 관계를 검증할 수 있다.
보안 구축 계획서 작성하기	3.1 보안 범위와 보안 아키텍처 설계서를 근거로 하여 구축 인력 및 장비를 배정할 수 있다. 3.2 배정된 내용에 따라 구축일정 지연과 품질, 성능에 대한 관리계획을 수립할 수 있다. 3.3 보안 범위, 보안 아키텍처 설계서, 관리계획 등을 포함하여 보안 구축 계획서를 작성할 수 있다.

- 평가시 고려사항

평가시 고려사항	<ul style="list-style-type: none"> • 보안 기능 분류 및 분석 능력 • 보안 기능에 따른 필요한 자원 관리 능력 • 일정 계획 수립 능력 • 보안 통제요소 확인 및 검증 능력 • 정보보호관리체계 인증 지침과 개인정보보호관리체계 인증지침 세부 내용 • 관리적, 기술적, 물리적 보안 범위 및 경계 설정 능력 • 관리 계획 수립 능력 • 구축 인력 및 장비 배정 능력 • 보안 구축 계획서 작성 능력
----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 지식 · 기술 · 태도

구 분	주 요 내 용
지식	<ul style="list-style-type: none"> • 관리계획 항목에 대한 지식 • 국내 정보보호 관련 법 • 보안 구축 계획서 작성 항목에 대한 지식 • 보안 기능에 대한 지식 • 보안 아키텍처 설계 지식 • 보안 아키텍처 설계서에 대한 지식 • 보안 통제요소에 대한 지식 • 요구공학 • 일정관리기법 • 자원관리기법 • 정보보호 관련법
기술	<ul style="list-style-type: none"> • 구축 범위 설정 능력 • 구축 일정 지연과 품질, 성능에 대한 관리계획 수립 능력 • 문서 작성 프로그램 활용 능력 • 보안 구축 계획서 작성 능력 • 보안 기능 분석 능력 • 보안 기능간의 상호관계 검증 능력 • 보안 통제요소 도출 능력 • 보안 통제요소 상호관계 분석 및 설계 능력 • 보안 통제요소 적용위치 산정 능력 • 아키텍처 설계서 분석 능력 • 일정 계획 수립 능력 • 자원 배정 능력 • 자원 산정 능력
태도	<ul style="list-style-type: none"> • 객관적인 시각으로 보안 기능을 분류 · 분석하려는 사고 • 관리계획을 구체적으로 수립하려는 태도 • 구축 인력 및 장비를 객관적이고 논리적으로 배정하려는 노력 • 꼼꼼하게 구축 일정 계획을 수립하려는 의지 • 모든 활동에 보안요구사항 준수 • 세밀하게 보안 통제요소를 세분화하려는 노력 • 세심하게 구축 범위를 설정하려는 노력 • 세심하게 기능 간의 상호관계를 설계하려는 노력 • 자산 누락을 방지하기 위해 적극적으로 필요한 자원 분석하려는 태도 • 적극적으로 상호관계를 분석하려는 태도 • 정해진 규칙에 따라 상호관계를 검증하려는 의지

- 장비

장 비 명	단 위	활용구분(공용/전용)	1대당 활용인원
• 컴퓨터	대	공용	1
• 문서작성 도구	개	공용	1

※ 장비는 주장비만 제시한 것으로 그 외의 장비와 공구는 별도로 확보

- 재료

재 료 목 록
• 해당없음

※ 자료는 주제료만 제시한 것으로 그 외의 자료는 별도로 확보

○ 과정/과목명 : 2001020603_18v4 보안 구축 요구사항 분석

- 훈련개요

훈련목표	보안 구축 요구사항 분석이란 사용자의 관리적, 물리적, 기술적 보안요구사항을 확인, 명세화하고 요구사항의 오류를 검증하는 능력을 함양.
수 준	5수준
훈련시간	30시간
훈련가능시설	컴퓨터실
권장훈련방법	원격훈련, 집체훈련 실습

- 편성내용

단 원 명 (능력단위 요소명)	훈 련 내 용 (수행준거)
보안요구사항 분석하기	1.1 사용자 요구사항을 분석하기 위하여 보안요구사항의 분석 절차를 정의할 수 있다. 1.2 사용자 요구사항의 관리적, 물리적, 기술적 타당성을 분석할 수 있다. 1.3 사용자 요구사항의 우선순위 정의를 위해 관리적, 물리적, 기술적 중요도를 정할 수 있다. 1.4 사용자 요구사항의 중요도에 따라 보안요구사항의 우선순위를 정할 수 있다.
보안요구사항 명세화하기	2.1 분석된 요구사항에 따라 보안요구사항의 구체화하기 위해 보안요구사항을 분류할 수 있다. 2.2 분류된 기본 요구사항에 따라 보안요구사항 우선순위의 타당성 검토를 위한 구체화 작업을 할 수 있다. 2.3 정제된 기본 요구사항에 대한 명세화를 위해 우선순위의 타당성을 검토할 수 있다. 2.4 구체화된 보안요구사항을 정의된 명세서 산출물 형식에 따라 문서를 작성할 수 있다.
보안요구사항 검증하기	3.1 명세화된 요구사항의 오류를 검증하기 위한 검증기준과 절차를 정의할 수 있다. 3.2 정의된 보안요구사항 검증 기준과 절차에 따라 보안요구사항의 오류를 검증할 수 있다. 3.3 보안요구사항의 오류 검증에 의해 보안요구사항을 협의하여 수정할 수 있다.

- 평가시 고려사항

평가시 고려사항	<ul style="list-style-type: none"> • 정보보호 요구사항의 수집과 도출 능력 • 정보보호 요구사항의 분석 능력 • 정보보호 요구사항의 명세화 능력 • 정보보호 요구사항의 오류 검증 능력 • 평가된 위험에 대한 걱정 대응 능력 • 소프트웨어 공학과 요구공학의 숙지 • PMBOK(Project Management Body of Knowledge) 기본 지식
----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 지식 · 기술 · 태도

구 분	주 요 내 용
지식	<ul style="list-style-type: none"> • PMBOK(Project Management Body of Knowledge) • 소프트웨어 개발방법론 • 소프트웨어공학과 요구공학 • 정보보호 요구사항 검증 기법 • 정보보호 요구사항 명세화를 위한 품질관리지식 • 정보보호 요구사항 분석기법 • 정보보호 요구사항 분석을 위한 통계기법 • 정보보호 요구사항 타당성 분석기법
기술	<ul style="list-style-type: none"> • 정보보호 요구사항 관리 도구 사용 기술 • 정보보호 요구사항 관리를 위한 문서작성 도구 활용 기술 • 정보보호 요구사항 분석 기술(통계 분석, 타당성 분석) • 정보보호 요구사항 정리 및 분류 기술
태도	<ul style="list-style-type: none"> • 객관적이고 분석적으로 사고하려는 태도 • 목표하는 보안 시스템의 기능과 성능향상을 위한 노력 • 정보보호 요구분석 기준과 절차 준수 • 정보보호 요구사항 정의를 위한 품질관리 절차 준수 • 조직의 보안환경과 보안기술을 지속적으로 숙지하려는 노력

- 장비

장 비 명	단 위	활용구분(공용/전용)	1대당 활용인원
• 컴퓨터	대	공용	1
• 문서작성 도구	개	공용	1

※ 장비는 주장비만 제시한 것으로 그 외의 장비와 공구는 별도로 확보

- 재료

재 료 목 록
• 해당없음

※ 재료는 주제료만 제시한 것으로 그 외의 재료는 별도로 확보

○ 과정/과목명 : 2001020604_18v4 관리적 보안 구축

- 훈련개요

훈련목표	관리적 보안 구축이란 정보보호 정책을 수립하고, 이를 시행 및 유지관리 할 수 있는 정보보호조직을 구성하여, 조직의 인적보안을 관리하는 능력을 함양.
수 준	6수준
훈련시간	40시간
훈련가능시설	컴퓨터실
권장훈련방법	집체훈련 실습

- 편성내용

단 원 명 (능력단위 요소명)	훈 련 내 용 (수행준거)
정보보호정책 수립하기	<ol style="list-style-type: none"> 1.1 조직의 보안요구사항에 따라 정보보호 활동을 규정한 정보보호정책과 정책 시행을 위한 지침, 절차, 매뉴얼로 구분하여 제정할 수 있다. 1.2 정기적인 정보보호정책 및 정책 시행문서의 타당성 검토를 통해, 정보보호 정책에 미치는 영향을 분석하고 필요한 경우 개정 할 수 있다. 1.3 정보보호정책 및 정책시행 문서에서 정한 정보보호 활동 수행을 통해 운영 기록을 생성하여 유지 할 수 있다.
정보보호조직 구성하기	<ol style="list-style-type: none"> 2.1 정보보호 정책시행 위해 조직의 규모, 업무 중요도에 따라 정보보안 조직을 구성할 수 있다. 2.2 정보보호 관련법에서 요구하는 정보보호 최고책임자와 정보보호 관련 담당자의 역할 및 책임을 정의할 수 있다. 2.3 정보보호 최고책임자와 정보보호 관련 담당자의 활동을 평가할 수 있는 체계를 수립할 수 있다.
인적보안대책 수립하기	<ol style="list-style-type: none"> 3.1 조직 내 중요 정보자산을 취급하는 직무를 정의하고 해당 직무를 수행하는 주요 직무자를 지정할 수 있다. 3.2 직무의 권한 오남용을 예방하기 위해 정보보호 관련 직무 분리 기준을 수립을 통해 직무별 역할과 책임을 지정 할 수 있다. 3.3 중요정보를 취급하는 주요 직무자는 최소한으로 지정하고 주기적으로 주요 직무자 현황을 관리할 수 있다. 3.4 임직원의 퇴직 및 직무변경 시 인사부서와 정보보호 및 시스템 운영 관련 부서에서 이행해야 할 자산반납, 접근권한 회수·조정, 결과 확인 절차를 수립할 수 있다.

- 평가시 고려사항

평가시 고려사항	<ul style="list-style-type: none"> • 정보보호정책 및 정책시행 문서(지침, 절차) 수립 능력 • 정보보호 및 개인정보보호 관련 법률 숙지 및 이해 능력 • 정보보호 관련 조직 실무구성 능력 • 내·외부 인적보안 관리 능력
----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 지식 · 기술 · 태도

구 분	주 요 내 용
지식	<ul style="list-style-type: none"> • 개인정보 보호법 • 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(ISMSP) • 정보보호관리체계에 관한 국제 표준 규격(ISO27001) • 정보통신망 이용촉진 및 정보보호 등에 관한 법률
기술	<ul style="list-style-type: none"> • 문서에 대한 형상관리 능력 • 인사 관리 능력 • 정보보호 및 개인정보보호 관련 법률 이해 능력 • 조직 구성 능력
태도	<ul style="list-style-type: none"> • 법적 준거성을 준수하려는 노력 • 요구사항을 모든 판단과 활동의 기준으로 하는 태도 • 주어진 절차를 준수하려는 태도 • 주어진 현상의 근본 원인을 파악하려는 노력

- 장비

장 비 명	단 위	활용구분(공용/전용)	1대당 활용인원
• 컴퓨터	대	공용	1
• 문서작성 도구	개	공용	1

※ 장비는 주장비만 제시한 것으로 그 외의 장비와 공구는 별도로 확보

- 재료

재 료 목 록
• 해당없음

※ 재료는 주제료만 제시한 것으로 그 외의 재료는 별도로 확보

○ 과정/과목명 : 2001020605_18v3 물리적 보안 구축

- 훈련개요

훈련목표	물리적 보안 구축이란 물리적 보호구역을 지정하고, 시스템을 보호하며, 사무실 보안을 구축하는 능력을 함양.
수 준	3수준
훈련시간	40시간
훈련가능시설	컴퓨터실
권장훈련방법	집체훈련 실습

- 편성내용

단 원 명 (능력단위 요소명)	훈 련 내 용 (수행준거)
물리적 보호구역 통제하기	<ol style="list-style-type: none"> 1.1 주요 설비 및 시스템을 보호하기 위하여 업무의 중요도 및 정보자산 위치에 따라 업무관련 공간을 물리적 보호구역으로 지정할 수 있다. 1.2 지정된 물리적 보호구역에 대해 보호구역별 특성에 따라 물리적 보호 대책을 수립할 수 있다. 1.3 수립된 물리적 보호 대책에 따라 필요한 설비를 충분히 갖추고 운영절차를 수립할 수 있다. 1.4 수립된 운영절차에 따라 인가된 사람만이 출입할 수 있도록 출입을 통제하고 출입 이력을 관리할 수 있다.
시스템 보호하기	<ol style="list-style-type: none"> 2.1 서버, 네트워크 장비, 백업장치 등 정보시스템 특성에 따라 시스템을 분리하여 배치할 수 있다. 2.2 보안사고 발생 시 신속한 조치를 위하여 시스템의 물리적 위치를 확인할 수 있는 방안을 마련할 수 있다. 2.3 외부로부터 물리적 손상을 입거나 전기적 영향을 받지 않도록 전력 및 통신 케이블을 보호할 수 있다.
사무실 보안 구축하기	<ol style="list-style-type: none"> 3.1 일상 업무를 수행하는 사무실의 개인업무 및 공용업무 환경에 대한 사무실 보안 정책을 수립할 수 있다. 3.2 수립된 사무실 보안 정책에 따라 개인업무 및 공용업무 환경 보안을 수행할 수 있다. 3.3 개인업무 및 공용업무 환경에 대한 보안 준수 여부를 주기적으로 점검할 수 있다.

- 평가시 고려사항

평가시 고려사항	<ul style="list-style-type: none"> • 정보보호 및 개인정보보호 관련 법률 숙지 및 이해 능력 • 물리적 보호구역 출입 통제 능력 • 외부 영향으로부터의 시스템 보호 및 신속한 조치 능력 • 개인업무 및 공용업무 환경 보안 점검 능력
----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 지식 · 기술 · 태도

구 분	주 요 내 용
지식	<ul style="list-style-type: none"> • 개인정보 보호법 • 네트워크 이론 • 방송통신설비의 기술기준에 관한 규정 • 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(ISMSP) • 정보보호관리체계 국제표준(ISO/IEC 27001) • 정보통신망 이용촉진 및 정보보호 등에 관한 법률 • 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조(집적된 정보통신시설의 보호)
기술	<ul style="list-style-type: none"> • 건축 도면 판독 능력 • 네트워크 구축 능력 • 사무기기 활용 능력 • 시스템 구성 능력
태도	<ul style="list-style-type: none"> • 고객 요구사항을 모든 판단과 활동의 기준으로 하는 태도 • 주어진 절차를 준수하려는 태도 • 주어진 현상의 근본 원인을 파악하려는 노력

- 장비

장 비 명	단 위	활용구분(공용/전용)	1대당 활용인원
• 컴퓨터	대	공용	1
• 문서작성 도구	개	공용	1

※ 장비는 주장비만 제시한 것으로 그 외의 장비와 공구는 별도로 확보

- 재료

재 료 목 록
• 해당없음

※ 재료는 주재료만 제시한 것으로 그 외의 재료는 별도로 확보

○ 과정/과목명 : 2001020610_18v4 보안인증 관리

- 훈련개요

훈련목표	보안인증 관리란 조직이 정보보호 관리체계를 구축·운영하고 있을 때, 보안인증기준에 적합한지를 인증기관으로 하여금 객관적이고 독립적인 평가를 통해 적합성 여부를 검증받는 능력을 함양.
수 준	6수준
훈련시간	40시간
훈련가능시설	컴퓨터실
권장훈련방법	집체훈련 실습

- 편성내용

단 원 명 (능력단위 요소명)	훈 련 내 용 (수행준거)
보안인증 준비하기	1.1 보안 인증 절차에 따라 인증 취득 계획을 수립 할 수 있다. 1.2 보안 인증에서 요구하는 통제항목에 따라 관리적, 기술적, 물리적 관리체계를 구축 할 수 있다. 1.3 구축된 관리적, 기술적, 물리적 보안 관리 활동에 따른 증적자료를 산출, 유지관리 할 수 있다.
보안인증 신청하기	2.1 보안 인증 신청 절차에 따라 인증 신청서를 작성하고, 제출서류를 준비, 제출 할 수 있다. 2.2 보안 인증 수수료 기준에 따라 수수료를 산출 할 수 있다. 2.3 인증기관으로부터 보안 인증 제출서류를 기반으로 서면 심사에 대응 할 수 있다.
보안인증 심사받기	3.1 보안인증 절차에 따라 인증심사 기관으로 부터 통보된 심사 계획을 접수 할 수 있다. 3.2 보안인증 심사계획에 따라 인증 심사 대응 조직을 구성하고, 인증 관련 서류를 준비 할 수 있다. 3.3 보안인증 현장심사 시 심사원의 인터뷰 질의, 현장 실사 활동에 대응 할 수 있다.
보안인증 부적합사항 조치하기	4.1 인증기관의 인증 심사결과에 따라 보안 인증 규격 대비 결함 사항에 대해 접수 할 수 있다. 4.2 보안 인증 결함사항에 대해 조치계획을 수립하고, 시정 조치를 할 수 있다. 4.3 시정 조치 확인 절차에 따라 인증기관의 결함 조치 확인에 대응 할 수 있다.
보안인증 사후관리하기	5.1 인증 취득 후 보안 인증 요건에 따라 인증 체계를 운영, 유지관리 할 수 있다. 5.2 보안 인증 유지를 위해 인증 사후 심사를 신청, 대응 할 수 있다. 5.3 보안 인증 갱신을 위해 인증 갱신 심사를 신청, 대응 할 수 있다.

- 평가시 고려사항

평가시 고려사항	<ul style="list-style-type: none"> • 정보보호 및 개인정보보호 관련 법률분석 능력 • 보안인증 규격 분석 능력 • 보안인증체계를 수립·운영하는 방법과 절차 수행 능력
----------	-----------------------------------------------------------------------------------------------------------------------------------------------

- 지식 · 기술 · 태도

구 분	주 요 내 용
지식	<ul style="list-style-type: none"> • ISO27001인증규격 • 보안인증체계를 수립 · 운영하는 방법과 절차 • 정보보호 관리체계 인증 등에 관한 고시 • 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(ISMSP) • 정보보호관리체계에 관한 국제 표준 규격(ISO27001) • 정보통신망 이용촉진 및 정보보호 등에 관한 법률
기술	<ul style="list-style-type: none"> • 보안인증 규격 분석 능력 • 보안인증체계를 수립 · 운영하는 방법과 절차 수행 능력 • 비용산정 능력 • 의사소통 능력 • 정보보호 및 개인정보보호 관련 법률분석 능력
태도	<ul style="list-style-type: none"> • 법적 준거성을 준수 하려는 노력 • 보안 인증 규격을 준수하려는 태도 • 보안 인증 절차를 준수하려는 태도 • 보안인증 결함을 수용하고, 적극적으로 개선하려는 태도

- 장비

장 비 명	단 위	활용구분(공용/전용)	1대당 활용인원
• 컴퓨터	대	공용	1
• 문서작성 도구	개	공용	1

※ 장비는 주장비만 제시한 것으로 그 외의 장비와 공구는 별도로 확보

- 재료

재 료 목 록
• 해당없음

※ 재료는 주제료만 제시한 것으로 그 외의 재료는 별도로 확보

○ 과정/과목명 : 2001020611_18v4 소프트웨어 개발 보안 구축

- 훈련개요

훈련목표	소프트웨어 개발 보안 구축이란 정의된 보안요구사항에 따라 SW의 보안 요구사항을 명세하고 이에 따라 SW에 대한 보안을 설계, 구현, 테스트하는 능력을 함양.
수 준	5수준
훈련시간	40시간
훈련가능시설	컴퓨터실
권장훈련방법	집체훈련 실습

- 편성내용

단 원 명 (능력단위 요소명)	훈 련 내 용 (수행준거)
소프트웨어 개발 보안 설계하기	1.1 정의된 보안요구사항에 따라 응용프로그램에 대한 보안 요구사항을 명세할 수 있다. 1.2 명세된 보안 요구사항을 만족하는 응용프로그램을 설계 할 수 있다. 1.3 보안성이 강화된 응용프로그램 구현을 위한 환경을 구축할 수 있다. 1.4 보안성이 강화된 응용프로그램 구현을 위한 일정 계획을 수립할 수 있다.
소프트웨어 개발 보안 구현하기	2.1 수립된 구현 계획에 따라 보안성이 강화된 응용프로그램을 구현할 수 있다. 2.2 구현된 응용프로그램의 결함 여부를 테스트할 수 있다. 2.3 테스트 결과에 따라 발견된 결함을 관리할 수 있다.

- 평가시 고려사항

평가시 고려사항	<ul style="list-style-type: none"> • SW개발 보안 요구사항에 맞는 보안의 구현 안전성 • 구현된 SW개발 보안에 대한 테스트 • 테스트 완료 후 도출되는 결함의 관리 및 추적
----------	-----------------------------------------------------------------------------------------------------------------------------------------------------

- 지식 · 기술 · 태도

구 분	주 요 내 용
지식	<ul style="list-style-type: none"> • CVE(Common Vulnerabilities and Exposures) • CWE(Common Weakness Enumeration) • Secure SDLC(Software Development Life Cycle) • 시큐어 코딩 • 시큐어 코딩(Secure Coding) • 식별 및 인증 • 암호 알고리즘 • 응용프로그램에 사용된 프로그래밍 • 접근 통제 • 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(ISMSP) • 정보보호관리체계에 관한 국제 표준 규격(ISO27001)
기술	<ul style="list-style-type: none"> • PC, 주변장치 등 설치 및 환경 구성 기술 • 관련 응용프로그램 설치, 보안패치 및 업그레이드 관련 기술 • 기술적 의사소통 능력 • 보안 Framework 작성 기술 • 보안 아키텍처 수립 기술 • 운영체제(OS) 설치 및 운용 능력 • 응용프로그램 실행 제어 기술 • 응용프로그램 환경 설정 기술 • 장애 발생 시 적절한 복구 조치 능력
태도	<ul style="list-style-type: none"> • 객관적인 테스트와 적극적인 문제해결 자세 • 보안요구사항 준수 • 설계된 응용프로그램 보안을 준수하여 구현하는 의지

- 장비

장 비 명	단 위	활용구분(공용/전용)	1대당 활용인원
• 컴퓨터	대	공용	1
• 문서작성 도구	개	공용	1

※ 장비는 주장비만 제시한 것으로 그 외의 장비와 공구는 별도로 확보

- 재료

재 료 목 록
• 해당없음

※ 재료는 주재료만 제시한 것으로 그 외의 재료는 별도로 확보

○ 과정/과목명 : 2001020612_18v4 데이터베이스 보안 구축

- 훈련개요

훈련목표	데이터베이스 보안 구축이란 정의된 보안요구사항에 맞게 데이터베이스를 분석하여 보안 요구사항을 명세하고 설계, 구현, 테스트하는 능력을 함양.
수 준	5수준
훈련시간	40시간
훈련가능시설	컴퓨터실
권장훈련방법	집체훈련 실습

- 편성내용

단 원 명 (능력단위 요소명)	훈 련 내 용 (수행준거)
데이터베이스 보안 설계하기	1.1 정의된 보안요구사항에 따라 데이터베이스에 대한 보안 요구사항을 명세할 수 있다. 1.2 명세된 보안 요구사항을 만족하는 데이터베이스를 설계 할 수 있다. 1.3 보안성이 강화된 데이터베이스 구현을 위한 환경을 구축할 수 있다. 1.4 보안성이 강화된 데이터베이스 구현을 위한 일정 계획을 수립할 수 있다.
데이터베이스 보안 구현하기	2.1 수립된 구현 계획에 따라 보안성이 강화된 데이터베이스를 구현할 수 있다. 2.2 구현된 데이터베이스의 결함 여부를 테스트할 수 있다. 2.3 테스트 결과에 따라 발견된 결함을 관리할 수 있다.

- 평가시 고려사항

평가시 고려사항	<ul style="list-style-type: none"> • 데이터베이스(DB) 보안 요구사항에 맞는 보안의 구현 안전성 • 구현된 데이터베이스(DB) 보안에 대한 테스트 • 테스트 완료 후 도출되는 결함의 관리 및 추적
----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

- 지식 · 기술 · 태도

구 분	주 요 내 용
지식	<ul style="list-style-type: none"> • 데이터베이스(DB)와 데이터베이스(DB)시스템 개념 • 식별 및 인증 • 암호 알고리즘 • 접근 통제 • 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(ISMSP) • 정보보호관리체계에 관한 국제 표준 규격(ISO27001) • 정보통신망 이용촉진 및 정보보호 등에 관한 법률
기술	<ul style="list-style-type: none"> • Database 계정 관리 기술 • Database 성능 개선 기술 • Database 암호화 기술 • Database 접근 제어 관리 기술 • 관리 시스템 접근통제 기술 • 데이터 베이스 취약점 분석 능력 • 데이터베이스 보안 기술 적용 능력 • 데이터베이스(DB) 시스템 사용 기술 • 로그 분석 도구 사용 기술 • 보안 Framework 작성 기술 • 보안 아키텍처 수립 기술
태도	<ul style="list-style-type: none"> • 객관적인 테스트와 적극적인 문제해결 태도 • 모든 활동에 보안요구사항 준수 • 설계된 데이터베이스(DB) 보안을 준수하여 구현하려는 노력

- 장비

장 비 명	단 위	활용구분(공용/전용)	1대당 활용인원
• 컴퓨터	대	공용	1
• 문서작성 도구	개	공용	1

※ 장비는 주장비만 제시한 것으로 그 외의 장비와 공구는 별도로 확보

- 재료

재 료 목 록
• 해당없음

※ 재료는 주재료만 제시한 것으로 그 외의 재료는 별도로 확보

○ 과정/과목명 : 2001020613_18v4 시스템 보안 구축

- 훈련개요

훈련목표	시스템 보안 구축이란 정의된 보안요구사항에 따라 시스템 보안 요구사항을 명세하고 설계, 구현, 테스트하는 능력을 함양.
수 준	5수준
훈련시간	40시간
훈련가능시설	컴퓨터실
권장훈련방법	집체훈련 실습

- 편성내용

단 원 명 (능력단위 요소명)	훈 련 내 용 (수행준거)
시스템 보안 설계하기	1.1 정의된 보안요구사항에 따라 시스템에 대한 보안 요구사항을 명세할 수 있다. 1.2 명세된 보안 요구사항을 만족하는 시스템을 설계 할 수 있다. 1.3 보안성이 강화된 시스템 구현을 위한 환경을 구축할 수 있다. 1.4 보안성이 강화된 시스템 구현을 위한 일정 계획을 수립할 수 있다.
시스템 보안 구현하기	2.1 수립된 구현 계획에 따라 시스템 보안을 구현할 수 있다. 2.2 구현된 시스템 보안의 결함 여부를 테스트할 수 있다. 2.3 테스트 결과에 따라 발견된 결함을 관리할 수 있다.

- 평가시 고려사항

평가시 고려사항	<ul style="list-style-type: none"> • 시스템 보안 요구사항에 맞는 보안의 구현 안전성 • 구현된 시스템 보안에 대한 테스트 • 테스트 완료 후 도출되는 결함의 관리 및 추적
----------	---------------------------------------------------------------------------------------------------------------------------------------------------

- 지식 · 기술 · 태도

구 분	주 요 내 용
지식	<ul style="list-style-type: none"> Platform 별 운영 체제 동작 메카니즘 서비스 공격 유형 시스템 보안 솔루션 종류 및 유형 별 제공 기능 시스템 아키텍처 식별 및 인증 암호 알고리즘 접근 통제 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(ISMSP) 정보보호관리체계에 관한 국제 표준 규격(ISO27001)
기술	<ul style="list-style-type: none"> 로그 분석 도구 사용 기술 보안 Framework 작성 기술 보안 솔루션 활용 기술 보안 아키텍처 수립 기술 서버 보안 소프트웨어 설치 및 운영 기술 서버, 운영체제 취약점 분석 능력 서버별 인증 접근통제 구현 관리 능력 운영체제별 보안설치 기술 운영체제의 환경 설정 기술
태도	<ul style="list-style-type: none"> 객관적인 테스트와 적극적인 문제해결 태도 모든 활동에 보안요구사항 준수 설계된 서버 보안을 준수하여 구현하려는 노력

- 장비

장 비 명	단 위	활용구분(공용/전용)	1대당 활용인원
• 컴퓨터	대	공용	1
• 문서작성 도구	개	공용	1

※ 장비는 주장비만 제시한 것으로 그 외의 장비와 공구는 별도로 확보

- 재료

재 료 목 록
• 해당없음

※ 재료는 주재료만 제시한 것으로 그 외의 재료는 별도로 확보

○ 과정/과목명 : 2001020614_18v4 네트워크 보안 구축

- 훈련개요

훈련목표	네트워크 보안 구축이란 정의된 보안요구사항에 따라 네트워크 보안 요구사항을 명세하고 설계, 구현, 테스트하는 능력을 함양.
수 준	5수준
훈련시간	40시간
훈련가능시설	컴퓨터실
권장훈련방법	집체훈련 실습

- 편성내용

단 원 명 (능력단위 요소명)	훈 련 내 용 (수행준거)
네트워크 보안 설계하기	1.1 정의된 보안요구사항에 따라 네트워크에 대한 보안 요구사항을 명세할 수 있다. 1.2 명세된 보안 요구사항을 만족하는 네트워크를 설계 할 수 있다. 1.3 보안성이 강화된 네트워크 구현을 위한 환경을 구축할 수 있다. 1.4 보안성이 강화된 네트워크 구현을 위한 일정 계획을 수립할 수 있다.
네트워크 보안 구현하기	2.1 수립된 네트워크 보안 구현 계획에 따라 네트워크 보안을 구현할 수 있다. 2.2 네트워크 보안 구현 결과에 대하여 테스트하고 테스트 결과를 관리할 수 있다.

- 평가시 고려사항

평가시 고려사항	<ul style="list-style-type: none"> • 네트워크 보안 요구사항에 맞는 보안의 구현 안전성 • 구현된 네트워크 보안에 대한 테스트 • 테스트 완료 후 도출되는 결함의 관리 및 추적
----------	-----------------------------------------------------------------------------------------------------------------------------------------------------

- 지식·기술·태도

구 분	주 요 내 용
지식	<ul style="list-style-type: none"> • 네트워크 QOS • 네트워크 개념 • 네트워크 기반 공격 유형 • 네트워크 보안 솔루션 • 네트워크 보안 프로토콜 • 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(ISMSP) • 정보보호관리체계에 관한 국제 표준 규격(ISO27001)
기술	<ul style="list-style-type: none"> • 네트워크 관리 프로그램 사용 기술 • 네트워크 사용자 관리 능력 • 네트워크 장비 사용 기술 • 네트워크 취약점분석 능력 • 로그 분석 도구 사용 기술 • 프로토콜 활용 능력
태도	<ul style="list-style-type: none"> • 객관적인 테스트와 적극적인 문제해결 태도 • 모든 활동에 보안요구사항 준수 • 설계된 네트워크 보안을 준수하여 구현하려는 노력

- 장비

장 비 명	단 위	활용구분(공용/전용)	1대당 활용인원
• 컴퓨터	대	공용	1
• 문서작성 도구	개	공용	1

※ 장비는 주장비만 제시한 것으로 그 외의 장비와 공구는 별도로 확보

- 재료

재 료 목 록
• 해당없음

※ 재료는 주제료만 제시한 것으로 그 외의 재료는 별도로 확보

Ⅲ. 고려사항

1. 활용방법

- 훈련기준에서 제시한 이외의 과정수립에 필요한 사항은 근로자직업능력개발법 등 관련 규정을 참고하시기 바랍니다.
- 본 훈련기준의 훈련과정은 모듈식으로, 장-단기과정 모두에서 활용가능하며, 훈련사업별로 요구하는 훈련과정 편성지침에 따라 편성할 수 있습니다.
- 3월 350시간 이상의 장기 훈련과정을 편성하는 경우, 수강생의 수준에 적합하게 훈련이수 체계도에서 제시한 해당직종의 훈련과정/과목을 필수로 반영하고, 이외 관련 직종의 과정/과목을 선택하여 편성할 수 있습니다.
 - * 단, 훈련생이 ‘필수과정’의 일부 훈련 과정/과목을 이수하거나, 직무수행경력이 있는 경우에는 해당 훈련과정/과목을 제외하고 훈련할 수 있습니다.
 - * 효율적으로 훈련하기 위해 둘 이상의 과정/과목을 결합하여 대(大)과목으로 편성하거나, 하나의 과정/과목을 둘 이상의 세(細)과목으로 편성하여 훈련할 수 있습니다.
 - * 훈련과정/과목에서 제시한 훈련시간은 훈련생의 학습능력을 고려하여 최대 50%까지 증감 조정하여 훈련할 수 있습니다.

2. 참고사항

가. 관련자격종목

- 정보보안기사
- 정보보안산업기사

나. 직업활동 영역

- 정보보호 전문기업
- 정보통신 관련 기업
- 정보보호 관련 정부·공공기관
- 일반 기업 정보보호 지원부서

다. 국가직무능력표준 관련 직종

- SW아키텍처
- IT품질보증
- IT테스트
- 기술영업
- 마케팅
- 응용SW엔지니어링
- 시스템엔지니어링
- DB엔지니어링
- NW엔지니어링
- UIUX엔지니어링
- IT시스템관리
- IT기술지원

○IT프로젝트관리

라. 관련 홈페이지 안내

- 훈련기준 및 국가직무능력표준 : <http://www.ncs.go.kr>
- 자격정보 : <http://www.qnet.or.kr>
- 훈련교재 및 매체 : <http://book.hrdkorea.or.kr>