1.1. 관리체계 기반마련

<table>
<tr><th colspan="2">정보보호 및 개인정보보호 위원회 회의록</th></tr>
<tr><td>설명</td><td>• 정보보호 및 개인정보보호 위원회 회의록은 경영진의 정보보호 및 개인정보보호 활동에 대한 의사결정을 확인할 수 있는 증적자료 중 하나로, 작성 시에는 '참석자', '회의일시', '회의 안건' 등을 회의에 관련된 사항을 상세히 작성하여야 한다.</td></tr>
<tr><td>관련 통제항목</td><td>1.1.1 경영진의 참여</td></tr>
<tr><td>인증기준</td><td>최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.</td></tr>
<tr><td colspan="2">
<u>정보보호 및 개인정보보호 위원회 회의록</u>

1. 회의정보

<table>
<tr><td>참석자</td><td colspan="2">강민구 이사(CPO), 차순영 부장(정보보안팀), 지영순 부장(인프라팀), 박민영 팀장(감사팀), 지영석 팀장(법무팀), 차민경 대리(정보보안팀)</td></tr>
<tr><td>회의일시</td><td colspan="2">20XX년 X월 X일</td></tr>
<tr><td rowspan="3">회의안건</td><td>1</td><td>개인정보보호 정책 지침 개정 사항 공표</td></tr>
<tr><td>2</td><td>신규 보안장비 도입 사업 추진 의결</td></tr>
<tr><td>3</td><td>내부 보안규정 위반자 징계 처리 의결</td></tr>
</table>
2. 회의내용

<table>
<tr><td>회의내용</td><td>
1. 개인정보보호 정책 지침 개정 사항 의결
- 개인정보보호 정책, 개인정보 처리방침, 개인정보 침해사고 대응 매뉴얼 등 정책·지침 3종 개정안의 주요 개정 사항 안내 (차순영 부장, 정보보안팀)
- 개인정보보호 정책 지침 개정 사항 법률 검토 결과 발표 (지영석 팀장, 법무팀)
- 개인정보보호 정책 지침 개정 의결, 2019년 1월 14일(월)자로 시행 예정 (강민구 이사, CPO)

2. 신규 보안장비 도입 사업 추진 의결
- 신규 보안장비(DDoS 보안장비, DB 접근제어 솔루션) 2종의 도입 필요성 발표 (차순영 부장, 정보보안팀)
- 신규 보안장비 도입(DB 접근제어 솔루션) 시 인프라팀 업무의 변동예상 사항 안내 (지영순 부장, 인프라팀)
- 신규 보안장비 사업 의결, 경쟁입찰 형식으로 추진 (강민구 이사, CPO)
- 2019년 2월 중 RFP 작성 및 사업 공고 예정 (차순영 부장, 정보보안팀)

3. 내부 보안규정 위반자 징계 처리 의결
- 내부 보안규정 위반자(인프라팀 박현중 사원)의 보안규정 위반사고 개요 설명 (박민영 팀장, 감사팀)
→ 사건개요 : 인프라팀 A 대리는 개발 편의를 위하여 별도의 보고절차 없이 OO 시스템의 실 데이터를 개발 중인 신규 업무포털의 테스트 데이터로 무단사용
- 내부 인사규정에 의거, 감봉 3개월 처분 (강민구 이사, CPO)
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th colspan="2">정보보호 최고책임자 지정 내역</th></tr>
<tr><td>설명</td><td>• 정보보호 최고책임자 지정 내역은 조직의 정보보호 최고책임자 지정 현황을 확인할 수 있는 증적자료 중 하나로, 작정보보호 최고책임자는 인사발령 등을 통하여 공식적으로 임명하여야 하며, 당연직의 경우 정보보호 및 개인정보보호 정책서에 그 직위를 명시하여야 한다.</td></tr>
<tr><td>관련 통제항목</td><td>1.1.2 최고책임자의 지정</td></tr>
<tr><td>인증기준</td><td>최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.</td></tr>
<tr><td colspan="2">
OO 업체

수 신 전사
(경 유)
제 목 OO 업체 정보보호 최고책임자 변경

OO 업체 정보보호 최고책임자가 아래와 같이 변경되었음을 통보하여 드립니다.

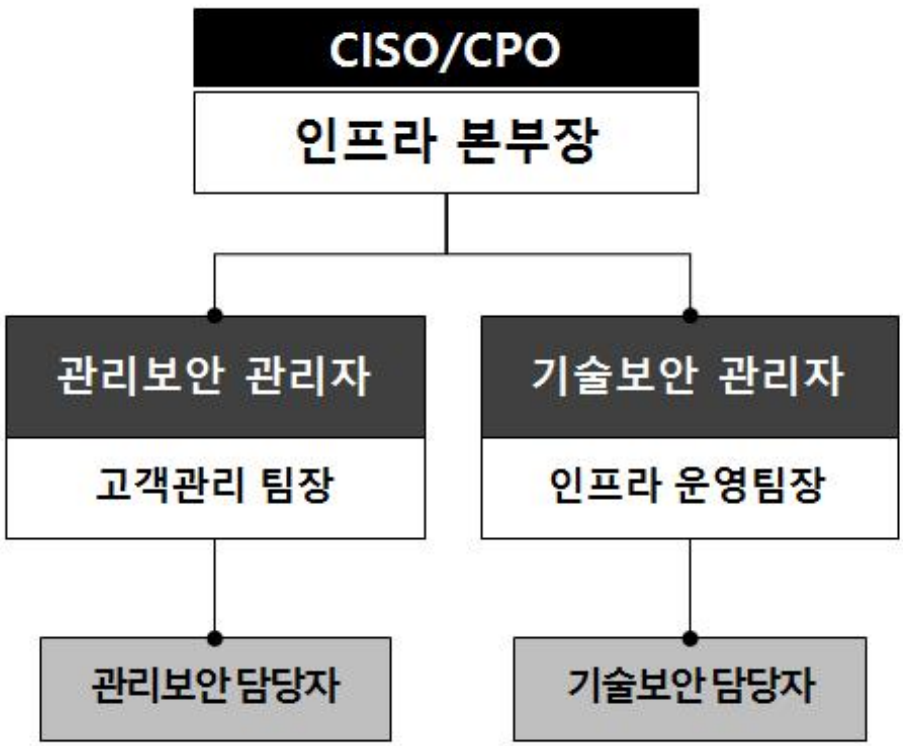
- 아 래 -

- 정보보호 최고책임자
<table>
<tr><th>구분</th><th>소속</th><th>직위</th><th>성명</th><th>변경사유</th><th>변경일자</th></tr>
<tr><td>이전</td><td>인프라본부</td><td>본부장(이사)</td><td>강현태</td><td rowspan="2">인사이동</td><td>20XX.XX.XX.자</td></tr>
<tr><td>신규</td><td>인프라본부</td><td>본부장(이사)</td><td>장형기</td><td>20XX.XX.XX.자</td></tr>
</table>
끝.

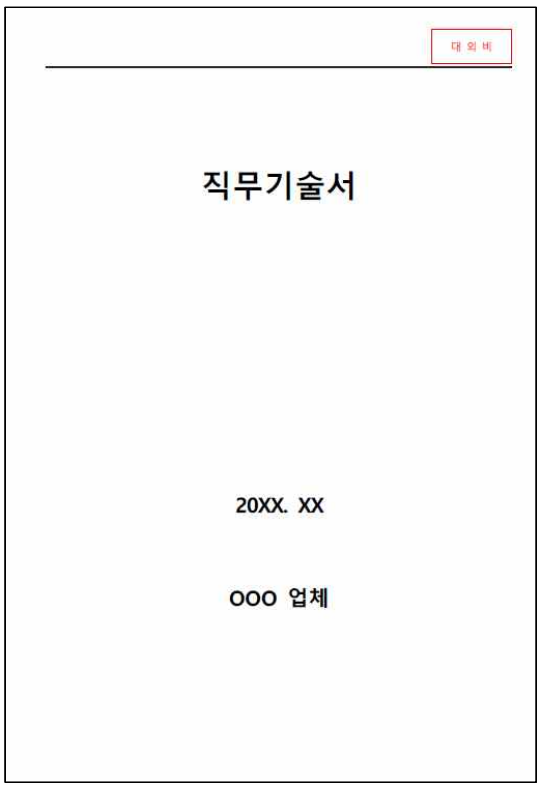
o o 업 체 대 표 이 사

<table>
<tr><td>담당자</td><td>박가연</td><td>정보보호팀장</td><td>남규태</td><td>인사팀장</td><td>서민국</td><td>인프라본부장</td><td>장형기</td></tr>
<tr><td>대표이사</td><td>차순영</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

정보보호 및 개인정보보호 조직도	
설명	• 정보보호 및 개인정보보호 조직도는 조직의 개인정보보호 인력구성 현황을 확인할 수 있는 증적자료 중 하나로, 작성 시 정보보호 및 개인정보보호 주요 직무자(CISO, CPO 등)의 현황이 확인되어야 한다.
관련 통제항목	**1.1.3 조직 구성**
인증기준	**최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.**



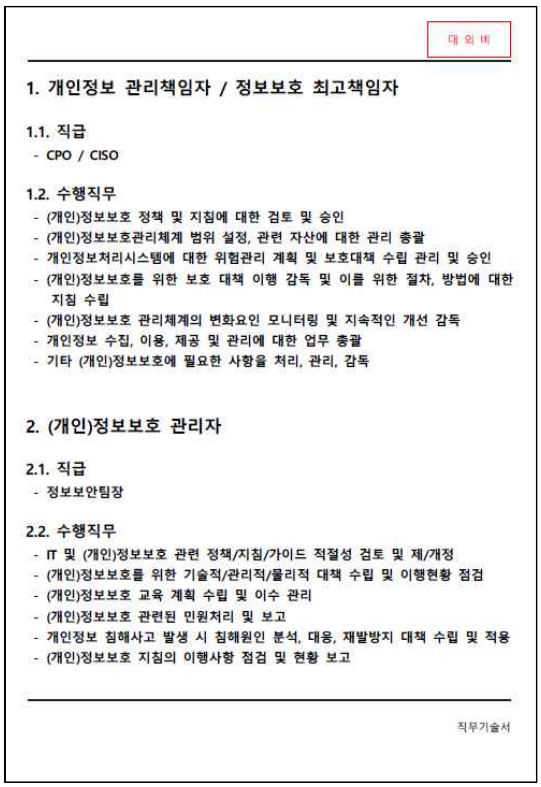
직무기술서	
설명	• 직무기술서는 조직 내 개인정보보호 인력의 직무현황을 확인할 수 있는 증적자료 중 하나로, 정보보호 및 개인정보보호 관련 담당자 및 부서별 담당자 등 실무자의 정보보호 및 개인정보보호 관련 직무를 문서화 하여야 한다.
관련 통제항목	**1.1.3 조직 구성**
인증기준	**최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.**


대 외 비

직무기술서

20XX. XX

OOO 업체


대 외 비

1. 개인정보 관리책임자 / 정보보호 최고책임자

1.1. 직급
- CPO / CISO

1.2. 수행직무
- (개인)정보보호 정책 및 지침에 대한 검토 및 승인
- (개인)정보보호관리체계 범위 설정, 관련 자산에 대한 관리 총괄
- 개인정보처리시스템에 대한 위험관리 계획 및 보호대책 수립 관리 및 승인
- (개인)정보보호를 위한 보호 대책 이행 감독 및 이를 위한 절차, 방법에 대한 지침 수립
- (개인)정보보호 관리체계의 변화요인 모니터링 및 지속적인 개선 감독
- 개인정보 수집, 이용, 제공 및 관리에 대한 업무 총괄
- 기타 (개인)정보보호에 필요한 사항을 처리, 관리, 감독

2. (개인)정보보호 관리자

2.1. 직급
- 정보보안팀장

2.2. 수행직무
- IT 및 (개인)정보보호 관련 정책/지침/가이드 적절성 검토 및 제/개정
- (개인)정보보호를 위한 기술적/관리적/물리적 대책 수립 및 이행현황 점검
- (개인)정보보호 교육 계획 수립 및 이수 관리
- (개인)정보보호 관련된 민원처리 및 보고
- 개인정보 침해사고 발생 시 침해원인 분석, 대응, 재발방지 대책 수립 및 적용
- (개인)정보보호 지침의 이행사항 점검 및 현황 보고

직무기술서

정보보호 및 개인정보보호 관리체계 범위 정의서	
설명	• 정보보호 및 개인정보보호 관리체계 범위 정의서는 정보보호 및 개인정보보호 관리체계의 범위를 확인할 수 있는 증적자료 중 하나로, 작성 시 관리체계 범위에는 사업(서비스)과 관련된 임직원, 정보시스템, 정보, 시설 등 유·무형의 핵심자산이 누락 없이 포함되어야 한다.
관련 통제항목	**1.1.4 범위 설정**
인증기준	**조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 개인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서화하여야 한다.**

II 인증의 범위

□ 전체 서비스(사업) 현황

① 인증희망 이유

인증희망 이유	☞ 법적요구, 고객요구, 내부 방침 등 고려사항을 기술		
의무대상 여부	기준	사유	의무대상자만 작성

② 인증심사 담당자

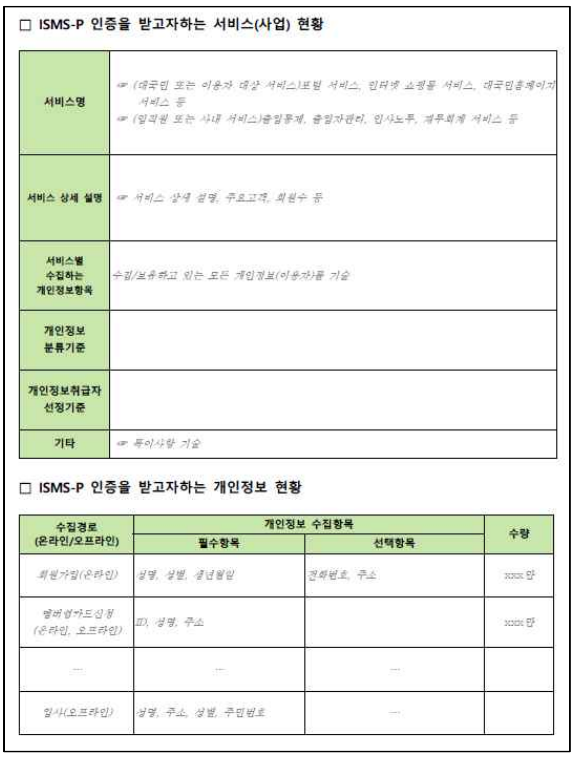
직급(업무)	부서	성명/직호	연락처	이메일	ISMS	ISMS-P
CISO, 개인정보보호 책임자	정보보호관리본부	홍길동 이사	01-1234-1234	abc@_____.kr	O	O
정보보호 책임자	정보보호관리실	성춘향	01-1234-1234	abc@_____.kr		
정보보호 담당자	정보보호관리팀	이몽룡	01-1234-1234	abc@_____.kr		
정보보호 담당자	정보보호관리팀					

③ 현재 제공 중인 전체 서비스(사업)

☞ 인증범위 포함여부와 상관없이 신청인이 제공하는 전체 서비스를 모두 기술

No	서비스명	서비스설명 및 URL	인증범위 포함여부	제외사유
1	㈜고성시대 홈쇼핑 쇼핑몰		ISMS-P	-
2	㈜고성 대표 홈페이지		ISMS	-
3	㈜고성 그룹웨어		N	내부망 전용 서비스
4			N	

- 1 -



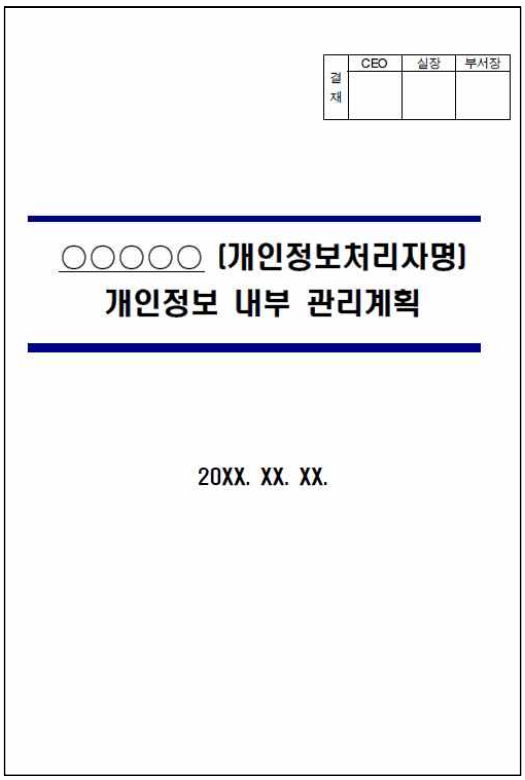
□ ISMS-P 인증을 받고자하는 서비스(사업) 현황

서비스명	☞ (대국민 또는 이용자 대상 서비스)보험 서비스, 인터넷 쇼핑몰 서비스, 대국민홈페이지 서비스 등 ☞ (임직원 또는 사내 서비스)출입통제, 출입자관리, 인사노무, 재무회계 서비스 등
서비스 상세 설명	☞ 서비스 상세 설명, 주요고객, 회원수 등
서비스별 수집하는 개인정보항목	수집/보유하고 있는 모든 개인정보(이용자를 기술
개인정보 분류기준	
개인정보취급자 선정기준	
기타	☞ 특이사항 기술

□ ISMS-P 인증을 받고자하는 개인정보 현황

수집경로 (온라인/오프라인)	개인정보 수집항목		수량
	필수항목	선택항목	
회원가입(온라인)	성명, 성별, 생년월일	전화번호, 주소	xxxx 만
멤버쉽카드신청 (온라인, 오프라인)	ID, 성명, 주소		xxxx 만
...	...	...	
입사(오프라인)	성명, 주소, 성별, 주민번호	...	

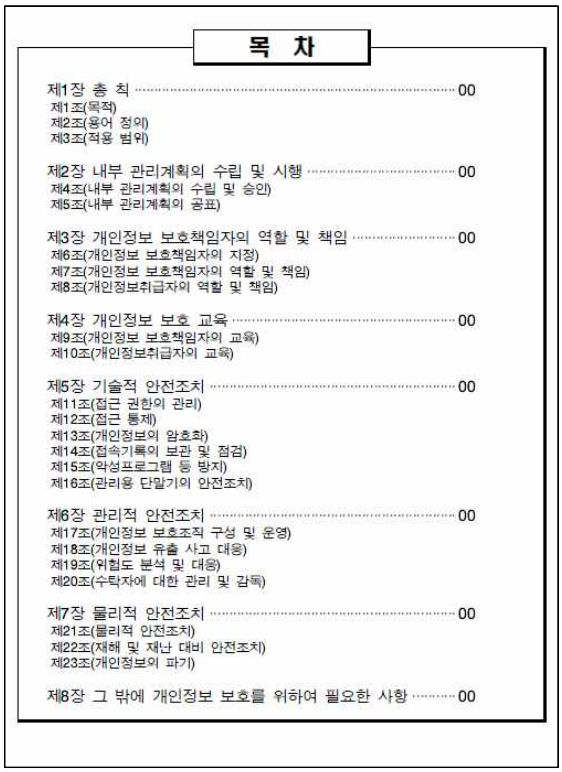
내부관리계획	
설명	• 내부관리계획은 조직의 개인정보보호 정책을 확인할 수 있는 증적자료 중 하나로, 개인정보보호법 및 정보통신망법 등 관련 법규에서 요구되는 사항을 포함하여 수립 및 시행하여야 한다.
관련 통제항목	**1.1.5 정책 수립**
인증기준	**정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.**



결재	CEO	실장	부서장

○○○○○ (개인정보처리자명)
개인정보 내부 관리계획

20XX. XX. XX.



목 차

정보보호 및 개인정보보호 투자 내역	
설명	• 정보보호 및 개인정보보호 투자 내역은 조직의 정보보호 및 개인정보보호 관리체계의 효과적 구현과 운영을 위해 필요한 예산을 지원하는지 확인할 수 있는 증적자료 중 하나로, 최고경영자는 매년 관리체계의 구축 및 운영을 위해 필요한 예산과 자원을 평가 및 지원하여야 한다.
관련 통제항목	**1.1.6 자원 할당**
인증기준	**최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.**

< OO 업체 20XX년도 정보보호 예산 투자 내역 >

구분	투자 사항	예산	담당부서/담당자	시기
솔루션	망분리 솔루션 도입	100,000,000원	정보보호팀/강희순 팀장	2/4분기 예정
	서버용 백신 도입	53,000,000원	정보보호팀/강희순 팀장 정보인프라팀/지영태 대리	2/4분기 예정
	기존 정보보호 솔루션 유지보수 비용	10,000,000원	정보보호팀/강희순 팀장 정보인프라팀/지영태 대리	연중 상시
컨설팅	ISMS-P 인증 컨설팅 (최초심사)	100,000,000원	정보보호팀/강희순 팀장	4/4분기 예정
기타	개인정보보호 온라인 교육	5,000,000원	정보보호팀/강희순 팀장	3/4분기 예정

1.2. 위험 관리

정보자산 및 개인정보 자산분류 기준	
설명	• 정보자산 및 개인정보 자산분류 기준은 자산목록의 분류기준을 확인할 수 있는 증적자료 중 하나로, 조직 특성에 맞게끔 분류기준을 수립하여야 한다.
관련 통제항목	**1.2.1 정보자산 식별**
인증기준	**조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.**

자산분류 기준

※ 자산 코드 = 대분류-중분류-번호
(ex. 서버-리눅스-01 = SVR-LX-01)
자산분류 기준
대분류 : 일반적 ISMS-P 자산분류에 따라 시스템별 구분
중분류 : 대분류 내 항목 중 특징을 이루는 그룹단위별 구분
번호 : 임의에 따라 차례대로 순서 부여

대분류		중분류		설명
서버(SerVeR)	SVR	리눅스(LinuX)	LX	온라인 도서 판매 시스템을 운영하기 위한 컴퓨터 자원으로 Linux, Windows 등 OS기준으로 구분함
네트워크(NetWork)	NW	스위치(SWitCh)	SWC	전산시스템의 통신을 위해 필요한 자원으로 L2, L3 스위치 등 장비특성을 기준으로 구분함
데이터베이스(DataBase)	DB	SQL	SQL	전산시스템내 데이터를 관리하기 위한 자원으로 SQL, Oracle 등 OS 기준으로 구분함
보안장비(SecuritySystem)	SS	SS	SS	회사 내 전산자원을 보호하기 위한 자원으로 방화벽, IPS, 보안 솔루션 등 장비특성을 기준으로 구분하며 SW를 함께 포함함
WEB/WAS	WEB/WAS	Apache	APH	온라인 도서 판매 시스템을 제공하기 위한 자원으로 Apache, Tomcat 등 WEB/WAS 기준으로 구분함
		Tomcat	TMC	
어플리케이션(APPlication)	APP	WEB	WEB	전산시스템을 이용한 서비스를 제공하는 자원으로 Web, Mobile 등 서비스 형태를 기준으로 구분함
소프트웨어 (SoftWare)	SW	서버용(SerVeR)	SVR	전산시스템에 특정 목적을 수행하기 위해 설치된 자원으로 서버용, 사무용 등 설치장소를 기준으로 구분함
		사무용(OFFice)	OFF	
PC(PC)	PC	구매관리 본부(PURchase)	PUR	전산시스템에 접근 가능한 PC자원으로 PC소유주의 부서를 기준으로 구분함
		마케팅 본부(MarKeTing)	MKT	
		고객관리 본부(CUStomer)	CUS	
		인프라 본부(INFRa)	IFR	
		물류관리 본부(DiSTribution)	DST	
데이터(DATa)	DAT	로그(LOG)	LOG	회사 운영에 필요한 데이터로 보안 시스템 로그, 개인정보 등 데이터의 특성을 기준으로 구분함
		개인정보(PRIVacyInformation)	PRV	
설비(FAcility)	FA	전산실(Data Processing Room)	DPR	전산시스템의 물리적 안전을 위해 운영되는 자원으로 설비의 특성을 기준으로 구분함
		본사(HeaD Office)	HD	

자산평가 기준

※ 자산 등급(Asset Value) = 기밀성(1~3)+무결성(1~3)+가용성(1~3)
※ 자산 등급 평가기준
1등급 : 기밀성 + 무결성 + 가용성의 합이 8 ≦ X ≦ 9 인 경우
2등급 : 기밀성 + 무결성 + 가용성의 합이 5 ≦ X ≦ 7 인 경우
3등급 : 기밀성 + 무결성 + 가용성의 합이 3 ≦ X ≦ 4 인 경우

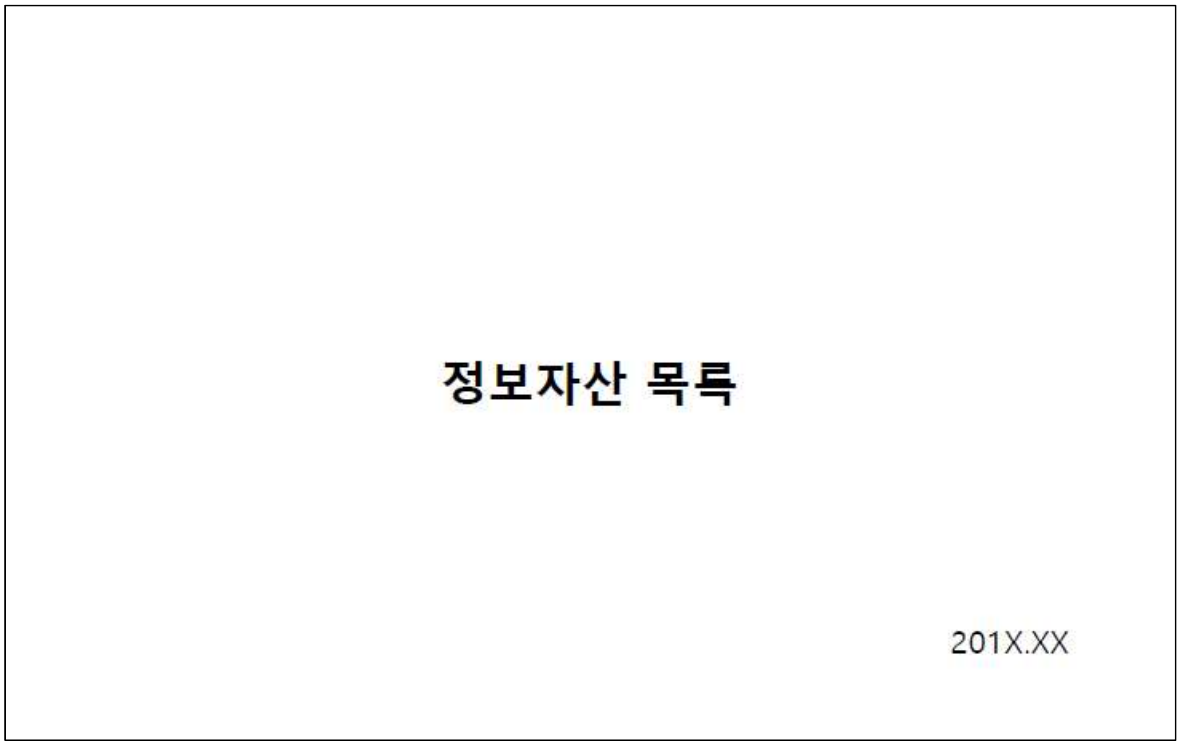
구분	등급	가치	설명
기밀성	상	3	중대한 재무적 손실이나 전사적 업무차질이 발생
	중	2	부분적 업무차질이나 간접적인 재무손실이 발생
	하	1	해당 사건을 무시할 수 있거나, 거의 영향을 미치지 않음
무결성	상	3	중대한 재무적 손실이나 전사적 업무차질이 발생
	중	2	부분적 업무차질이나 간접적인 재무손실이 발생
	하	1	해당 사건을 무시할 수 있거나, 거의 영향을 미치지 않음
가용성	상	3	업무의 차질이 1시간 이하로 발생
	중	2	업무의 차질이 1시간 ~ 24시간 발생
	하	1	업무의 차질이 24시간 이상 발생

자산등급 표

구분	등급	설명
기밀	1	회사 운영과 직접적인 관련이 있으며, 유출될 경우 영업을 중지하거나 벌금 이상의 처벌이 가해져 심각한 피해가 예상되는 정보자산
대외비	2	회사 운영과 간접적인 관련이 있으며, 유출될 경우 대외 신용의 하락이나 향후 운영에 약간의 지장이 발생 가능한 다소 피해가 예상되는 정보자산 (단, 외부 발표용 자료는 대외비로 한다.)
일반	3	회사의 운영과 관련이 있으며, 유출되어도 회사에 미치는 영향이 비미한 정보 자산

정보자산 및 개인정보 자산목록

설명	• 정보자산 및 개인정보 자산목록은 관리체계 내 자산현황을 확인할 수 있는 증적자료 중 하나로, 관리체계 범위 내의 자산을 식별하여 자산명, 용도, 위치, 책임자 등을 포함하여 목록화 관리하여야 한다.
관련 통제항목	**1.2.1 정보자산 식별**
인증기준	**조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.**



1. 서버

NO	구분	코드	자산명	IP	Hostname	모델명	OS/Ver	Vendor	용도
1	서버-리눅스 (SVR-LX)	SVR-LX-01	SAMPLE WEB/WAS 서버	*.*.*.*	SB_WEBWAS	x3250 M4	CentOS release 6.6	IBM	SAMPLE 홈페이지 WEB/WAS 서버
2		SVR-LX-03	회원 DB	*.*.*.*	CUS_DB	x3250 M4	Ubuntu 16.04 LTS	IBM	SAMPLE 홈페이지 고객 정보 저장
3		SVR-LX-04	주문/배송 DB	*.*.*.*	ORD_DB	x3250 M4	Ubuntu 16.04 LTS	IBM	주문 및 배송 정보 저장
4		SVR-LX-05	재고 DB	*.*.*.*	IVT_DB	x3250 M4	Ubuntu 16.04 LTS	IBM	도서 재고 관리
5		SVR-LX-07	콜센터 DB	*.*.*.*	CALL_DB	x3250 M4	Ubuntu 16.04 LTS	IBM	고객 응대 내용 기록
6		SVR-LX-06	데이터 분석 DB	*.*.*.*	PRF_DB	x3250 M4	Ubuntu 16.04 LTS	IBM	고객 맞춤 추천 서비스 활용
7		SVR-LX-08	사용자 DB	*.*.*.*	EMP_DB	x3250 M4	Ubuntu 16.04 LTS	IBM	전자결재를 위한 사용자 정보 저장

NO	위치		관리자	책임자	자산가치평가			자산가치 등급	비고
	센터	랙번호			C	I	A		
1	10F 전산실	A-8	고애신	최유진	3	3	3	1등급	
2	10F 전산실	A-5	고애신	최유진	3	3	3	1등급	
3	10F 전산실	A-5	고애신	최유진	3	3	3	1등급	
4	10F 전산실	A-5	고애신	최유진	2	3	3	1등급	
5	10F 전산실	A-5	고애신	최유진	3	3	2	1등급	
6	10F 전산실	A-5	고애신	최유진	3	3	1	2등급	
7	10F 전산실	A-5	고애신	최유진	3	3	1	2등급	

개인정보 흐름표(ISMS-P 인증인 경우)

설명	• 개인정보 흐름표는 조직의 개인정보 처리업무 흐름을 확인할 수 있는 증적자료 중 하나로, 관리체계 범위 내의 개인정보 처리현황 분석하여 이를 처리단계 별로 업무 흐름을 분류 후 표 형태로 작성·보유하여야 한다.
관련 통제항목	**1.2.2 현황 및 흐름분석**
인증기준	**관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.**

(OOO 업체) 수집 흐름표

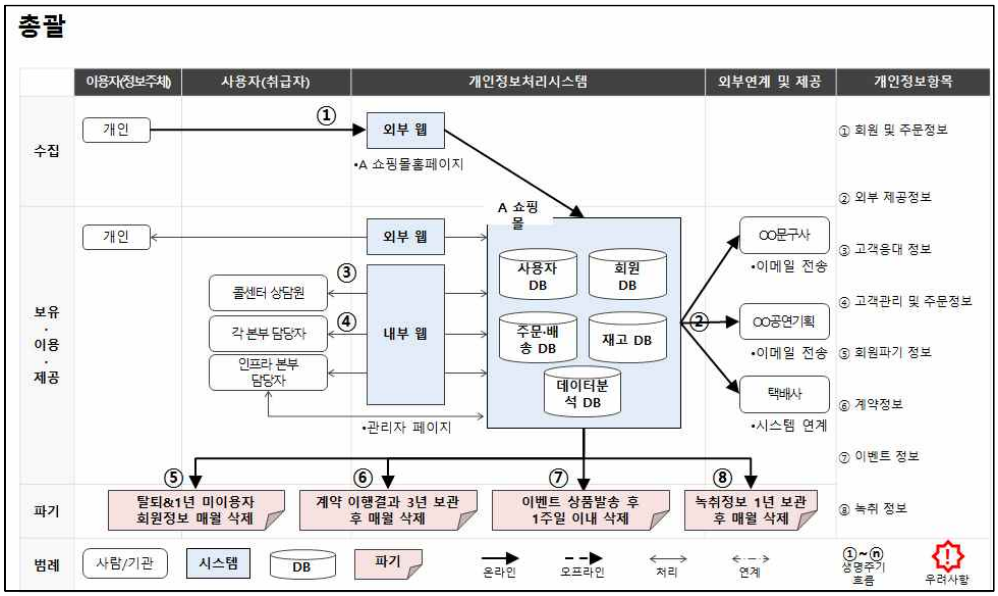
No	업무	상세 업무	수집 항목	수집 경로	수집 대상	수집 주기	수집 담당자	수집 근거	비고
1	회원관리	회원가입 및 탈퇴	(필수)ID, PW, 이름, 휴대폰 번호 (선택)생년월일, 성별, 주소, 직업	온라인-홈페이지	홈페이지 회원	상시	고객관리 본부 / 회원관리 담당자	정보주체의 동의	
2		고객 응대	(필수)휴대폰 번호, 녹취정보	전화	콜센터 문의 고객	상시	고객관리 본부 / 콜센터 직원	정보주체의 동의	
7	마케팅 활용	이벤트 관리	(필수)이름, 휴대폰 번호	온라인-홈페이지	홈페이지 이용자	이벤트 개설기간 상시	고객관리 본부 / 이벤트 담당자	정보주체의 동의	
8	홈페이지 관리	홈페이지 및 사용자 관리	해당사항 없음						

(OOO 업체) 보유이용 흐름표

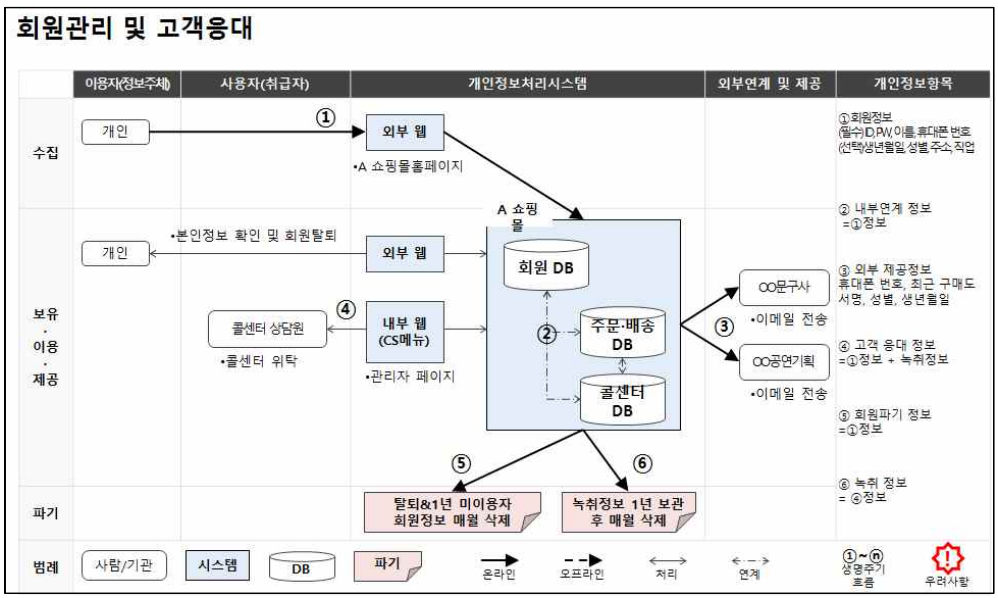
No	업무	상세 업무	보유형태	암호화 항목	이용목적	개인정보 취급자	이용 방법	비고
1	회원관리	회원가입 및 탈퇴	회원 DB	해당없음	회원가입 및 탈퇴현황 관리	고객관리 본부 / 회원관리 담당자	홈페이지 관리자페이지 접근	
2		고객 응대	콜센터 DB	해당없음	회원 문의 및 민원응대	고객관리 본부 / 콜센터 직원	홈페이지 관리자페이지 접근	
3	물류 및 구매관리	주문 및 배송 관리	주문/배송 DB	해당없음	도서구매요청에 대한 주문 및 배송추적 관리	물류관리 본부 / 주문배송 직원	홈페이지 관리자페이지 접근	
5	마케팅 활용	데이터 분석	데이터 분석 DB	해당없음	고객맞춤 서비스 동의회원에 대한 도서목록 추천	고객관리 본부 / 데이터 관리 담당자	홈페이지 관리자페이지 접근	
7		이벤트 관리	회원 DB	해당없음	이벤트 응모자에 관리	마케팅 본부 / 이벤트 담당자	홈페이지 관리자페이지 접근	

개인정보 흐름도(ISMS-P 인증인 경우)	
설명	• 개인정보 흐름도는 조직의 개인정보 처리업무 흐름을 확인할 수 있는 증적자료 중 하나로, 개인정보 흐름표를 기반으로 이를 도식화 한 문서 형태로 작성·보유하여야 한다.
관련 통제항목	**1.2.2 현황 및 흐름분석**
인증기준	**관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.**

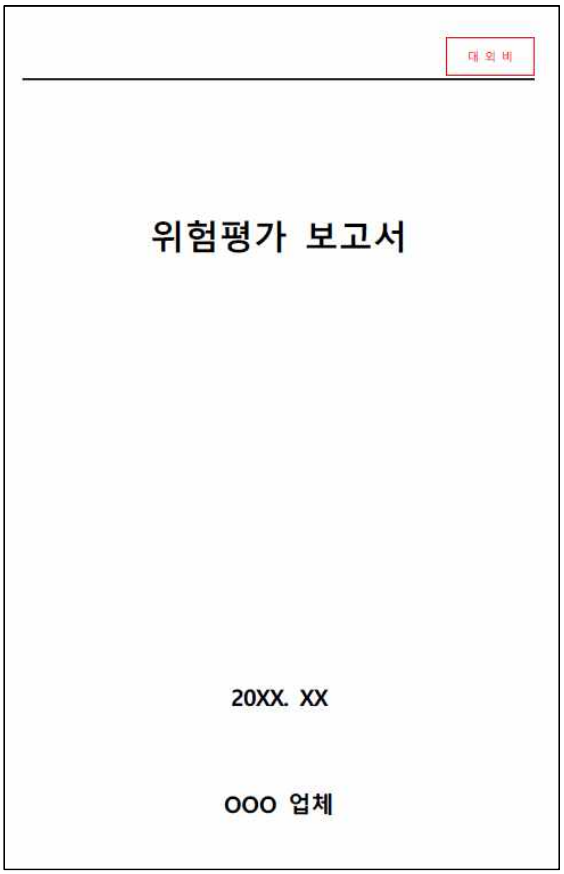
총괄



회원관리 및 고객응대



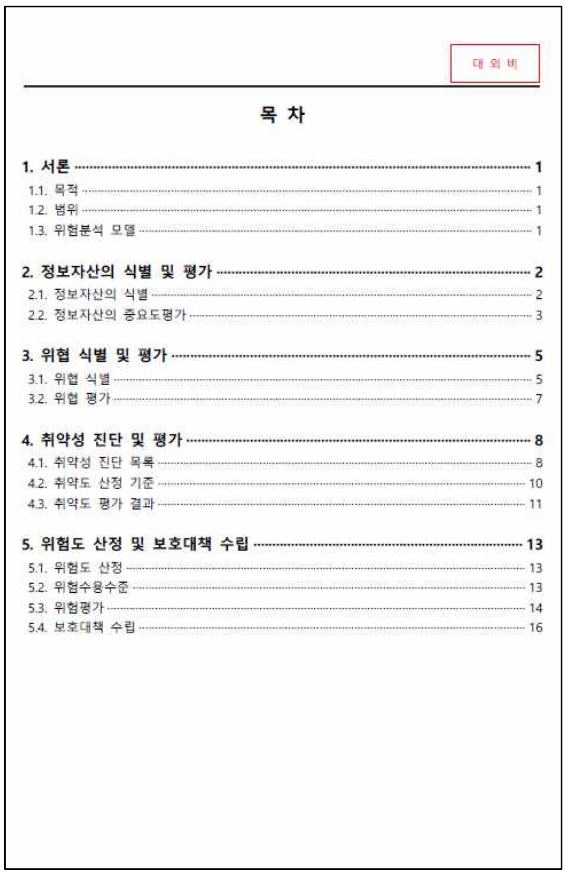
위험평가 결과보고서	
설명	• 위험평가 결과보고서는 조직의 위험 식별 여부를 확인할 수 있는 증적 자료 중 하나로, 관리적, 기술적, 물리적, 법적 분야 등 다양한 측면에서 발생할 수 있는 위험평가 결과를 문서화하여야 한다.
관련 통제항목	**1.2.3 위험 평가**
인증기준	**조직의 대내외 환경분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.**


대 외 비

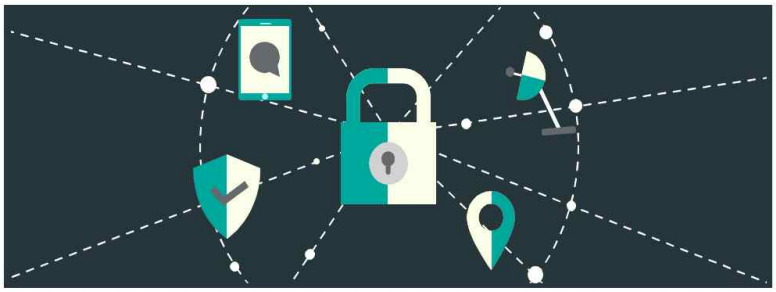
위험평가 보고서

20XX. XX

OOO 업체


대 외 비

목 차

<table>
<tr><th colspan="2">정보보호 및 개인정보보호 마스터플랜</th></tr>
<tr><td>설명</td><td>• 정보보호 및 개인정보보호 마스터플랜은 식별된 위험에 따른 보호대책을 확인할 수 있는 증적자료 중 하나로, 식별된 위험에 대한 처리전략(위험감소, 위험회피 등)을 수립하고 전략에 따른 적절한 정보보호 및 개인정보보호 대책을 포함하여야 한다.</td></tr>
<tr><td>관련 통제항목</td><td>1.2.4 보호대책 선정</td></tr>
<tr><td>인증기준</td><td>위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.</td></tr>
<tr><td colspan="2">


OOO 업체

(개인)정보보호 마스터플랜

2. 핵심과제 선정

핵심과제 도출
<table>
<tr><th>ISMS-P 통제번호</th><th>대책</th><th>설명</th><th>긴근성</th><th>적용성</th><th>총점 및 적용시기</th></tr>
<tr><td>1.1.1</td><td>CISO 별도 지정</td><td>CISO의 업무는 타 업무와 중복되지 않도록 별도 직제를 구성하여 지정 필요</td><td>6</td><td>4</td><td>10(중기)</td></tr>
<tr><td>1.1.3</td><td>정보보호 전담 실무조직의 구성</td><td>정보보호 전담인력을 충원하고 정보보호 전담업무를 수행할 조직 신설필요</td><td>6</td><td>4</td><td>10(중기)</td></tr>
<tr><td>2.2.2</td><td>개발/운영 직무분리</td><td>개발인력, 운영인력은 별도 인원을 지정하여 임의 개발물이 운영환경에 반영되지 않도록 조치필요</td><td>6</td><td>4</td><td>10(중기)</td></tr>
<tr><td>2.11.3</td><td>실시간 관제</td><td>시스템 로그는 성능검사 이외 보안이상징후를 탐지할 수 있도록 실시간 보안관제 도입 필요</td><td>6</td><td>4</td><td>10(중기)</td></tr>
</table>
</td></tr>
</table>