|  |
| --- |
| **정보보호 관리체계 인증 신청 가이드라인 v1.8** |

**□ 법적 근거**

 o ｢정보통신망 이용촉진 및 정보보호 등에 관한 법률｣ 시행령 제47조

|  |
| --- |
| 제47조(정보보호 관리체계 인증의 방법·절차·범위 등) ① 법 제47조제1항 또는 제2항에 따라 정보보호 관리체계의 인증을 받으려는 자는 정보보호 관리체계 인증신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 사항에 대한 설명이 포함된 정보보호 관리체계 명세서(전자문서를 포함한다)를 첨부하여 인터넷진흥원, 법 제47조제6항에 따라 지정된 기관(이하 "정보보호 관리체계 인증기관"이라 한다) 또는 법 제47조제7항에 따라 지정된 기관(이하 "정보보호 관리체계 심사기관"이라 한다)에 제출하여야 한다.1. 정보보호 관리체계의 범위2. 정보보호 관리체계의 범위에 포함되어 있는 주요 정보통신설비의 목록과 시스템 구성도3. 정보보호 관리체계를 수립·운영하는 방법과 절차4. 정보보호 관리체계와 관련된 주요 문서의 목록5. 정보보호 관리체계와 관련된 국내외 품질경영체제의 인증을 취득한 경우에는 그 명세(이하 생략) |

 o ｢정보보호 관리체계 인증 등에 관한 고시｣ 제16조

|  |
| --- |
| 제16조(인증의 신청 등) ① 법 제47조제1항 또는 제2항에 따라 정보보호 관리체계 인증을 받으려는 자는 별지 제13호서식의 정보보호 관리체계 인증 신청서를 인터넷진흥원·인증기관 또는 심사기관에 제출하여야 한다.② 신청기관은 인증의 범위 및 일정 등을 인터넷진흥원·인증기관 또는 심사기관과 사전 협의하여 신청하여야 한다.③ 인터넷진흥원·인증기관 또는 심사기관은 제14조에 따른 인증 의무대상자가 사업자 등록일이 속한 분기가 끝나는 날의 1개월 전까지 인증 신청을 한 경우 인증심사를 우선적으로 처리할 수 있다. |

**□ 인증심사 절차**



 **※ 최초심사 경우, 신청서를 제출한 뒤 인증서 부여까지는 최소 20여 주가 필요하므로 이점 고려하시어 신청을 부탁드립니다.**

**□ 제출 서류**

 o 정보보호 관리체계 인증신청서

 o 정보보호 관리체계 명세서

 ※ 2개월 이상 구축․운영 사실 및 운영명세서 포함

 o 사업자등록증(또는 고유번호증) 1부

**□ 신청 방법 및 문의처**

 o 신청 방법 : 공문 제출을 통한 신청

 ※ 우편 또는 직접방문 접수도 가능하나, 18:00시 이후 접수 불가

 ※ 전자문서의 경우, 이메일 제출 가능(공문 및 제출 자료 포함)

o 접수 및 문의처 : kisa\_isms@kisa.or.kr

|  |  |  |
| --- | --- | --- |
|  | **< 인증 신청 제출 서류 >** |  |
|  |  |
|  1. 정보보호 관리체계 인증신청서 2. 정보보호 관리체계 명세서 - 정보보호 관리체계의 범위 - 주요 정보통신 설비의 목록과 시스템 구성도 - 정보보호 관리체계 수립․운영 방법 및 절차 - 정보보호 관리체계 관련 주요 문서 목록 - 국내외 품질경영체제 인증서 취득 명세- 정보보호 관리체계 인증 일부 심사기준 생략 명세서(의무대상자) - [별지] 정보보호 관리체계 운영명세서 3. 사업자등록증 (또는 고유번호증) |

|  |  |  |
| --- | --- | --- |
| 1 |  |  정보보호 관리체계 인증신청서 v1.8 |

|  |  |
| --- | --- |
| ■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제13호서식] <개정 2013.8.8.> |  |
| **정보보호 관리체계 인증 신청서** |
| ※ [ ]에는 해당되는 곳에 √표를 하고, 어두운 부분은 신청인이 작성하지 않습니다.  |
| 접수번호 |  | 접수일자 |  | 발급일 |  | 처리기간  |  |
|  |
| 신청인 | 업체명 | 사업자등록번호 |
| 주소 | 전화번호 |
| 대표자 |
|  |
| 인증신청의 구분 | [ ]최초심사[ ]사후심사[ ]갱신심사 |
| 정보보호 관리체계의 범위 | *※ 사후 심사의 경우, 기존 인증서內 인증범위명과 동일하게 작성* |
| 정보보호 관리체계의 범위에 포함되어 있는 종업원의 수 | *※ 종업원의 수 : 내부 및 외주 인력의 합산**※ p.8에 조직범위 총 인원수와 동일하게 작성* |
| 정보보호 관리체계의 범위에 포함되어 있는 서버의 수 | *※ 정보시스템 수 : 서버(웹서버, DB서버 등), 네트워크 장비(라우터, L4이상 스위치 등), 보안장비(방화벽, IDS, IPS, DDos 대응시스템, 웹방화벽 등)을 포함하여 산정**※ p.9에 작성한 수량과 동일하게 작성* |
|  |
|  「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제11항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계의 인증을 신청합니다. |
| 년 월 일 |
| 신청인(대표자)  |  (서명 또는 인) |
| **한국인터넷진흥원·인증기관 또는 심사기관** | 귀중 |
|  |
| 신청(신고)인제출서류 | 정보보호 관리체계 명세서 1부. | 수수료없음 |
| 담당공무원확인사항 | 법인사업자등록증 |
|  |
|  |
| 210mm×297mm[백상지(80g/㎡)] |

|  |  |  |
| --- | --- | --- |
| 2 |  |  정보보호 관리체계 명세서 |

|  |  |
| --- | --- |
| **작성 항목** | **기재 내용(요약)** |
| 1. 정보보호 관리체계의 범위 | ※ 인증을 받고자하는 서비스명과 정의 등을 기재 |
| 2. 정보보호 관리체계의 범위에 포함되어 있는 주요 정보통신설비의 목록과 시스템 구성도 | ※ 인증범위 대상과 제외 대상을 적시하고 그 사유를 기재 |
| 3. 정보보호 관리체계를 수립·운영하는 방법과 절차 | ※ 정보보호 관리체계 운영현황, 자산식별 기준, 취약점 점검 등에 관한 내용을 기재 |
| 4. 정보보호 관리체계와 관련된 주요 문서의 목록 | ※ 정보보호 관리체계 관련 주요 문서 목록을 기재 |
| 5. 정보보호 관리체계와 관련된 국내외 품질경영체제의 인증을 취득한 경우에는 그 명세 | ※ 현재 국내외 품질경영체계 인증을 취득하였을 경우, 인증서 명, 인증기관, 취득일 등을 기재 |

※ 위 표에는 주요 내용만을 기재하고, 세부 사항은 이후 페이지에 기재

|  |  |  |
| --- | --- | --- |
| **Ⅰ** |  | **정보보호 관리체계의 범위**(시행령 제47조제1항제1호) |

**□ 인증심사 진행 관련 정보**

 ① 인증심사 담당자

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 직급(업무) | 부서 | 성명 | 연락처 | 이메일 |
| CISO | 정보보호관리본부 | 홍길동 | 010-1234-1234 | *abc@\_\_\_\_\_\_\_\_\_.kr* |
| 정보보호 책임자 | 정보보호관리실 | 성춘향 | 010-1234-1234 | *abc@\_\_\_\_\_\_\_\_\_.kr* |
| 정보보호 담당자 | 정보보호관리팀 | 이몽룡 | 010-1234-1234 | *abc@\_\_\_\_\_\_\_\_\_.kr* |
| 정보보호 담당자 | 정보보호관리팀 |  |  |  |

 ② 인증심사 관련 컨설팅 업체 및 담당자 ( 업체/기간/담당자 ) : ㈜조선시대/15.01~15.06/김갑돌

※ ISMS인증심사 준비 시, 컨설팅 업체를 통하여 진행한 경우만 작성

 ③ 인증심사 희망일 및 인증심사장 장소

|  |  |  |  |
| --- | --- | --- | --- |
| 인증심사 희망일 | **15.00.00 ~ 00.00** | 인증심사장 장소 | 서울 송파구 중대로54 IT벤처타워 6층 회의실 |

 **※ 다수의 신청기관이 같은 날짜에 심사를 희망할 경우, 실제 인증심사일이 희망하는 날짜와 다를 수 있음**

**□ 전체 서비스(사업) 현황**

 ① 사업자 구분

|  |  |  |  |
| --- | --- | --- | --- |
| **인증희망 이유** |  *☞ 법적요구, 고객요구, 내부 정책 등 고려사항을 기술* | **의무대상 여부** | **Y/N** |
| **의무대상 기준** |  *☞ 예) 정보통신서비스 매출액 1000억원 / 방문자 540만명 / IDC사업자 / ISP사업자* ※ 의무대상기업만 작성 |
| **이용자(고객)** |  *☞ 개인(내국인, 외국인), 법인 등* | **회원수** | \_\_\_\_\_\_\_\_명 |

 ② 현재 제공 중인 전체 서비스(사업)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **서비스명** | **웹페이지** | **인증범위** **포함여부** | **제외사유** ※ 의무대상기업만 작성 |
| 1 | ㈜조선시대 홍길동 쇼핑몰 | * [http://www.aaa.com](http://www.xxx.com)
* <http://www.bbb.com>
* http://www.ccc.com
 | **Y** | - |
|  | ㈜고조선 그룹웨어 | * [http://www.ddd.com](http://www.xxx.com)
* [http://www.eee.com](http://www.bbb.com)
 | **N** | 내부망 전용 서비스 |
| 3 |  |  | **Y/N** |  |
| 4 |  |  | **Y/N** |  |

*☞ 인증범위 포함여부와 상관없이 신청기관이 제공하는 전체 서비스를 모두 기술*

 ③ 인증을 받고자 하는 서비스

|  |  |
| --- | --- |
| **서비스명** |  *☞ 포털 서비스, 통합정보리서비스, 대국민홈페이지서비스 등* |
| **서비스 설명 및 개인정보 포함여부** |  *☞ 각 서비스 별 상세 설명 및 개인정보 포함여부 표시* *※ 개인정보가 포함될 시 개인정보 유형 명시(이름, 이메일, 주소, 핸드폰 등)* |
| **웹페이지** |  *☞ 홈페이지 및 관련 서비스 웹페이지 URL 기술* |
| **관련 외주업체 활용현황** |  *☞ 위탁, 용역 수행업체 및 투입인력(xx명, 파견) 등 현황 기술* *☞ 서비스 관련 개발이나 운영 등을 위해 활용되는 외주업체 현황을 기술* |
| **기타** |  *☞ 특이사항 기술* |

③ 인력 및 물리적 위치

|  |  |  |  |
| --- | --- | --- | --- |
| **전체 인력** | xxx명(외주인력 포함) | **인증범위 내 인력** | xxx명(외주인력 포함) |
| **물리적 위치** | *명칭**(사업장명 또는 청사명)* | *위치* |
| *명칭* | *위치* |
| *명칭* | *위치* |

 ④ 전체 조직도 및 정보보호 조직도

|  |  |
| --- | --- |
| **전체 조직도** |  |
|  *☞ 신청기관의 전체 조직도를 삽입하고, 인증 범위에 해당하는 부서 표시* *☞ 부서별로 사업장 위치 등이 상이할 경우 상세 내용 기술* ***(예시)*** |
| **정보보호 조직도** |  |
|  *☞ 신청기관의 정보보호 조직도를 삽입하고, 정보보호관련 부서, 정보보호최고책임자, 정보보호책임자, 정보보호실무자, 정보보호위원회 등을 표기* *☞ CISO의 “부서 직책(직위)“를 함께 기재* *예) 경영관리본부 본부장(상무)* *☞ 정보보호위원회 구성원의 “부서 직책(직위)”를 함께 기재* *예) 구성원1 : 기획홍보실 실장(이사)* *구성원2 : 경영관리본부 본부장(상무)* *☞ 의사결정체를 확인할 수 있도록 구분* ***(예시)*** |
| **Ⅱ** |  | **주요 정보통신 설비의 목록과 시스템 구성도**(시행령 제47조제1항제2호) |

**□ 인증범위 대상**

 o 운영기간 : \_\_\_년 \_\_\_개월 (○○○○년 ○월 ~ ○○○○년 ○월)

 o 조직 범위

| **부서명(또는 용역업체명)** | **업 무** | **내부인력** | **외부인력****(용역포함)** | **합계** |
| --- | --- | --- | --- | --- |
| *인사팀* | *인적보안 및 교육* | xxx명 | xxx명 | xxx명 |
| *감사실* | *내부 보안감사* |  |  |  |
| *네트워크관리팀* | *네트워크 장비 및 보안장비 운영* |  |  |  |
| *…* | *…* |  |  |  |
| *…* | *…* |  |  |  |
| *…* | *…* |  |  |  |
|  **합 계** | xxx명 | xxx명 | xxx명 |

o 외부위탁 업무 현황 (자회사 포함)

| 구분 | 업체명 | 용역내용 | 상주여부 |
| --- | --- | --- | --- |
| 정보시스템 개발 |  |  | *Y/N* |
|  |  |  |
| 정보시스템 유지보수 |  |  |  |
|  |  |  |
| 서버운영 |  |  |  |
|  |  |  |
| NW운영 |  |  |  |
|  |  |  |
| 보안장비운영 |  |  |  |
|  |  |  |
| 보안관제 |  |  |  |
|  |  |  |
| 데이터센터 |  |  |  |
|  |  |  |
| 출입관리 및 경비 |  |  |  |
| 정보보호 컨설팅 |  |  |  |
| 기타 |  |  |  |

 o 시스템 및 서비스 범위(서비스별 분류하되 요약 작성)

| **서비스** | **구분** | **자산명****(어플리케이션 포함)** | **수량** | **용도 및 주요기능** | **자산위치** | **관리부서** |
| --- | --- | --- | --- | --- | --- | --- |
| *원격교육**서비스* | 서버 | *원격교육 웹서버* |  |  |  |  |
|  |  |  |  |  |
| 네트워크 |  |  |  |  |  |
| 보안장비 |  |  |  |  |  |
| PC |  |  |  |  |  |
| 어플리케이션 | 관리자 페이지 |  |  |  |  |
| … |  |  |  |  |  |
| *공통**인프라* |  |  |  |  |  |  |

 ※ 구분은 신청기관의 자산 분류기준에 따른 자산 유형과 일치해야 함

 o 전체 조직 및 시스템 중, 인증범위에 제외한 부서․시스템 목록 및 사유

| **구분** | **부서명(시스템구분)** | **대상 제외 사유** | **규모** |
| --- | --- | --- | --- |
| **부서(인력)** | *○○○팀* |  | xxx명 |
| … |  |  |
| **서비스** | *○○○서버* |  | xxx대 |
| … |  |  |

 o 물리적 범위 (위부위탁 포함)

| **사업장명** | **위치** | **관련부서** | **수행업무** | **상주인력** |
| --- | --- | --- | --- | --- |
|  | *서울 가락본동 대동빌딩* |  |  | *명* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**□ 시스템 및 네트워크 구성도**

|  |
| --- |
| EMB00000558263e*☞ 신청기관의 전체 시스템 및 네트워크 구성도를 명시하고, 인증 범위에 해당하는 부서 표시**☞ 시스템 및 구성도의 위치가 물리적으로 상이할 경우 상세 내용 기술* |

|  |  |  |
| --- | --- | --- |
|  | **< 작성 요령 >** |  |
|  |  |
| ※ 인증범위에 해당하는 서비스를 제공하기 위한 시스템과 네트워크 중심으로 작성하고, 다음 사항을 고려하여야 함 o 서버, 네트워크(라우터, 서비스), 보안시스템(방화벽, 침입탐지 등) 등을 포함 o 사무실, IDC, DMZ, VPN 구간에 대한 명시(해당 시) o IDC가 구분된 경우 해당 사항을 명시 o 시스템간의 네트워크 연결을 명시  |

**□ 정보보호 관리체계 인증범위 내 환경변화**

 ※ 사후/갱신심사 필수 작성, 최초심사의 경우 관련내용이 있는 경우에만 작성)

 o 조직(구성원) 환경 변화

 *☞ 전년대비 구성원 수 변경 현황 기술*

 *☞ 정보보호 최고책임자(CISO), 정보보호 책임자, 담당자 등의 변경 사항 기술*

 *☞ 조직구성 변경 사항 기술*

 o 정책/지침 개정 현황

 *☞ 정보보호 최고책임자(CISO), 정보보호 책임자, 담당자 등에 대한 전년도 대비 변경 현황 기술*

 o 주요 자산 변경 현황(신규도입, 용도변경, 폐기)

 *☞ 신규도입, 용도변경, 폐기된 범위 내 자산 현황 기술*

| **구분** | **자산내역** | **장비대 수** |
| --- | --- | --- |
| **신규도입** | *서버* | 대 |
| *네트워크* |  |
| *...* |  |
| **용도변경** |  |  |
|  |  |
| **폐기** |  |  |
|  |  |

 o 시스템/개발 환경변화(신규개발 등에 관한 변경사항)

 *☞ 시스템 환경(OS 변경 등)*

 *☞ 개발 환경에 대한 변화 (신규 시스템 개발, 전년도 개발 종료 등)*

 o 네트워크 환경변화

 *☞ 네트워크 구성 변경 사항에 대한 기술*

 o 물리적 환경변화

 *☞ 사무실, 전산실 등의 물리적인 위치 변경 사항 기술*

 o 외주용역 환경변화

 *☞ 신규용역, 용역해지 등의 변경 사항 기술*

|  |  |  |
| --- | --- | --- |
| **Ⅲ** |  | **정보보호 관리체계 수립ㆍ운영 방법 및 절차**(시행령 제47조제1항제3호) |

**□ 정보보호 규모 및 체계**

 o 정보보호 인력 및 예산 규모 - 전체 조직 및 비용(인증범위포함)

 - 정보보호 인력

(단위 : 명)

|  |  |  |
| --- | --- | --- |
| **회사內 전체 인력** | **IT 인력** | **정보보호 인력** |
| 명 | 명 | 명 |

 - 정보보호 예산

(단위 : %)

|  |  |
| --- | --- |
| **전체예산 대비 IT 예산** | **IT예산 대비 정보보호 예산** |
| *%*※ 비중(%)으로만 입력(금액으로 작성하지 말 것) | *%*※ 비중(%)으로만 입력(금액으로 작성하지 말 것) |

 o 홈페이지 등을 통한 정보보호 활동 내역 공개 여부(Y/N) :

**□ 정보보호 관리체계 운영현황**

 o 심사항목 및 운영명세서

|  |  |  |
| --- | --- | --- |
| **심사 영역** | **운영 현황** | **비고** |
| **통제 항목** | **심사 항목** |
| 관리과정 | 12 | 12 |  |
|  정보보호대책(13개 분야) | 1 | 6 |  |  |
| 2 | 4 |  |  |
| 3 | 3 |  |  |
| 4 | 3 |  |  |
| 5 | 4 |  |  |
| 6 | 5 |  |  |
| 7 | 9 |  |  |
| 8 | 10 |  |  |
| 9 | 2 |  |  |
| 10 | 14 |  |  |
| 11 | 22 |  |  |
| 12 | 7 |  |  |
| 13 | 3 |  |  |
| 계 | 92 | 0 |  |
|  합계 | 104 | 12 |  |

※ 상세 내용은 [[별지1]](#[별지1])(p.18)에 기재

※ 별지는 “ISMS 인증기준 세부점검항목”(자료실(ISMS) 37번)을 반드시 참고하여 작성

(http://isms.kisa.or.kr/kor/notice/dataView.jsp?p\_No=48&b\_No=48&d\_No=114&cgubun=&cPage=1&searchType=ALL&searchKeyword=)

 o 주요 정보보호 활동 목록(구축 운영 순서대로 작성)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **주요 활동** | **주기** | **담당자****(부서/성함)** | **실시유무****(O/X)** | **최근 실시** |
| *정보보호정책수립* | *1회/3년* | *홍길동/보안관리팀* | *O* | *2012.12월* |
| *백업훈련* | *1회/1년* | *홍길동/보안관리팀* | *O* | *2013.1월* |
| … |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **< 작성 요령 >** |  |
|  |  |
| ※ 정보보호 관리체계를 지속적으로 운영하기 위해서 주기적 또는 상시적으로 수행하는 정보보호 활동을 목록화하여 기재(주기, 담당자, 실시유무 등) |

 o 2개월 이상 구축․운영 증빙자료

|  |
| --- |
| ※ 증빙할 수 있는 승인문서, 계약서 등의 스캔 이미지 첨부※ 민감정보에 대해서는 마스킹 처리※ 문서명, 기관명, 주요내용 등을 포함 |

|  |  |  |
| --- | --- | --- |
|  | **< 작성 요령 >** |  |
|  |  |
| ※ 인증신청 2개월 전 운영날짜가 확인 가능한 관리적, 기술적 항목에 대한 운영증적(산출물) 1건씩 첨부 예)정보보호정책 또는 위험평가 승인문서, 백업정책 승인 문서 등 |

**□ 위험 관리**

 o 자산분류 기준

 ※ 자산을 분류한 유형을 기재. 예) S/W, 서버, 네트워크, 시설, 인력 등

 o 자산 중요도 산정방법

 ※ 자산 중요도 산정기준, 자산 등급 선정 계산방법 등을 기재 (자산 중요도 산정기준은 자산분류별로 상이할 수 있음)

 o 위험평가 방법론

 - 관리적, 기술적, 법적 위험 식별 방법

|  |  |  |
| --- | --- | --- |
| **구분** | **방법** | **산출물** |
| 관리적 위험 | *예) 베이스라인 접근법(체크리스트)* | *예) 분석결과* |
| 기술적 위험 | *예) 상세위험분석 방법* |  |
| 법적 위험 | *예) 베이스라인 접근(체크리스트)* |  |

 - 위험평가를 위한 위험도 산정기준

 - 수용 가능한 위험수준(DoA) 선정 방법

 o 위험관리 계획

 ※ 위험관리를 수행하기 위하여 인력 구성, 기간(단계별 구분), 대상, 방법, 예산 등을 구체화하여 기재

**□ 기술적 취약점 점검**

 o 취약점 점검 대상 선정방법 및 그 사유

 ※ 정보자산 중 취약점 점검으로 선정한 방법 및 그 사유를 기재

 o 취약점 점검 현황

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **기간****(○.○월~○월)** | **대상 서비스** | **대상 자산 및 규모** | **점검툴** | **취약점****(점검 시)** | **잔여취약점****(현재)** |
| *5개월**(2012.7월~11월)* | *웹서비스* | 서버 | 대 |  | 건 | 건 |
| 네트워크장비 | 대 |  | 건 | 건 |
| 보안장비 | 대 |  | 건 | 건 |
| PC | 대 |  | 건 | 건 |
| S/W | 대 |  | 건 | 건 |
| *…* | *…* |  | … | … |
| … |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **< 작성 요령 >** |  |
|  |  |
| ※ 최근 3년간 외부 정보보호 컨설팅업체를 통하여 취약점 점검을 받은 내용을 기재※ 취약점 : 취약점 점검 당시 발견된 취약점 건수※ 잔여 취약점 : 보완되지 않고 현재 남아 있는 취약점 건수 |

**□ 신청기관이 준수해야 할 법적 요구사항 현황**

|  |  |  |
| --- | --- | --- |
| **구분** | **관련 법적 요구사항** | **관련문서** |
| *예) 데이터센터 운영 서비스* | *예) 정보통신망법 제OO조* | *예) 정보보호정책 제O조(.....)* |
| *예) 정보통신망법 제OO조*  | *예) 정보보호정책 제O조(.....)* |
| *예) 집적정보 통신시설 보호지침 OO조* |  |
| *예) 전자정부법 제OO조* |  |
| … |  |
| … |  |  |

|  |  |  |
| --- | --- | --- |
|  | **< 작성 요령 >** |  |
|  |  |
| ※ 국내・외 법규에 의거하여 신청기관이 준수해야하는 법적 요구사항※ 관련문서 : 신청기관의 정책, 지침 등에 명시된 항목을 기재(세부조항번호까지 기재) |

**□ 내부감사 이력**

| **No.** | **기간**(년.월.일~월.일) | **수행 인력** | **감사결과 및 조치사항** |
| --- | --- | --- | --- |
| **부서****(또는 외주업체명)** | **성명** | **수행업무** |
| 1 | *3개월**(2012.2.1일**~2012.4.30일)* | *보안관리팀* | *홍길동* | *시스템개발 보안 점검* | … |
| *(조아컨설팅)* | *아무개* | *보안취약점 점검* | … |
| … | … | … | … |
| … | … | … | … | … | … |

※ 정보보호 관리체계(ISMS)가 효과적으로 운영되고 있는지 내부점검 수행

|  |  |  |
| --- | --- | --- |
| **Ⅳ** |  |  **정보보호 관리체계 관련 주요 문서 목록**(시행령 제47조제1항제4호) |

| **구분** | **문 서 명** | **관리****번호** | **주요 내용** | **제개정 주체****(부서/성명)** | **최근 재‧개정 일자** |
| --- | --- | --- | --- | --- | --- |
| **정책** | *정보보호정책* |  |  |  | *2014.04.26* |
| *개인정보보호정책* |  |  |  |  |
| *…* |  |  |  |  |
| **지침** | *정보보호조직관리지침* |  |  |  |  |
| *자산분류 및 관리지침* |  |  |  |  |
| *정보보호정책관리지침* |  |  |  |  |
| *서버보안관리지침* |  |  |  |  |
| *PC보안관리지침* |  |  |  |  |
| *사업연속성계획관리지침* |  |  |  |  |
| *아웃소싱보안지침* |  |  |  |  |
| *…* |  |  |  |  |
| **절차** | *보안성검토절차* |  |  |  |  |
| *문서보안관리절차* |  |  |  |  |
| *침해사고대응절차* |  |  |  |  |
| *서버보안관리절차* |  |  |  |  |
| *PC보안관리절차* |  |  |  |  |
| *백업관리절차* |  |  |  |  |
| *암호관리절차* |  |  |  |  |
| *…* |  |  |  |  |
| **기록****및****로그** | *임직원 보안서약서* |  |  |  |  |
| *출입 관리대장* |  |  |  |  |
| *정보보호 대책 명세서* |  |  |  |  |
| *…* |  |  |  |  |

※ 신청기관이 보유한 정보보호 관리체계 관련 문서 및 기록을 모두 기재

※ 위 표 “문서 명”은 단지 예시이며 해당 문서 명으로 존재해야 한다는 의미는 아님

|  |  |  |
| --- | --- | --- |
| **Ⅴ** |  |  **국내외 품질경영체제 인증서 취득 명세** (시행령 제47조제1항제5호) |

|  |  |  |  |
| --- | --- | --- | --- |
| **인증서명** | **인증기관** | **인증범위** | **유효기간** |
|  *ISO 27001* |  |  |  |
| *PIMS* |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Ⅵ** |  | **정보보호 관리체계 인증 일부 심사기준 생략 명세서**(망법 제47조제3항) |

**□ 법적 근거**

o ｢정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙｣ 제3조

|  |
| --- |
| **제3조(정보보호 관리체계 인증심사 일부의 생략)** ① 미래창조과학부장관은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) **제47조제2항에 따라 인증을 받아야 하는 자**가 다음 각 호의 어느 하나에 해당하는 **국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우**에는 같은 조 제3항에 따라 같은 조 제1항에 따른 **인증심사의 일부를 생략**할 수 있다.1. 「품질경영 및 공산품안전관리법」 제7조제2항에 따른 국제인정기관협력기구에 가입된 인정기관이 인정한 인증기관으로부터 받은 국제표준 정보보호경영시스템 인증2. 법 제47조의3 또는 「개인정보 보호법」 제13조제3호에 따른 개인정보보호 관리체계 인증3. 「정보통신기반 보호법」제9조에 따른 주요정보통신기반시설의 취약점 분석ㆍ평가② 제1항에 따라 정보보호 관리체계 인증심사의 일부를 생략하려는 경우에는 **다음 각 호의 요건을 모두 충족**하여야 한다.**1. 해당 국제표준 정보보호 인증 또는 정보보호 조치의 범위가 영 제47조제2항에 따른 정보보호 관리체계 인증의 범위와 일치할 것****2. 정보보호 관리체계 인증 신청 및 심사 시에 해당 국제표준 정보보호 인증이나 정보보호 조치가 유효하게 유지되고 있을 것**③ 법 제47조제3항에 따라 정보보호 관리체계 인증심사 일부의 생략을 받으려는 자는 인증심사 일부의 생략을 신청하는 서류에 국제표준 정보보호 인증서, 정보보호 조치 결과보고서 등 인증심사의 일부 생략 대상인 사실을 증명할 수 있는 서류를 첨부하여 제출하여야 한다. |

**□ 인증심사 생략대상 정보(규칙 제3조제1항)**

|  |  |
| --- | --- |
| **의무대상 여부** | *의무대상(정보통신매출 100억 이상)* |
| **국제표준 정보보호 인증 또는 정보보호 조치 정보(선택1)** |
| **국제표준 정보보호경영시스템 인증** | 인증번호 :  |
| 인증의 범위 :  |
| 인증유효기간 : . . ~ . .  | 인증기관 :  |
| 최근 인증심사 수행기간 : . . ~ . .  | 보완조치 완료일 : |
| **개인정보보호 관리체계 인증** | 인증번호 :  |
| 인증의 범위 :  |
| 인증유효기간 : . . ~ . .  | 인증기관 :  |
| 최근 인증심사 수행기간 : . . ~ . .  | 보완조치 완료일 : |
| **「정보통신기반 보호법」제9조에 따른 취약점의 분석ㆍ평가** | 기반시설 지정번호(공문번호) :  |  |
| 취약점 분석ㆍ평가 수행범위 :  |  |
| 취약점 분석ㆍ평가 수행기간 : . . ~ . . | 수행주체 :  |

※ 인증심사의 일부 생략 대상임을 확인할 수 있는 증빙자료 제출

- 국제표준 정보보호경영시스템 : 적용성보고서, 범위정의서, 정보보호 조치 결과서, 인증서(인증유지 공문) 등

- 개인정보보호관리체계 인증 : 운영명세서, 범위정의서, 보완조치내역서, 인증서(인증유지 공문) 등

- 「정보통신기반 보호법」제9조에 따른 취약점의 분석ㆍ평가 : 주요정보통신기반시설 보호대책서, 인증서(인증유지 공문)

**□ 인증심사 생략신청 정보(규칙 제3조제2항)**

**1. 인증심사 생략 범위 및 조직**

o 시스템 및 서비스 범위(서비스별 분류하되 요약 작성)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **서비스** | **구분** | **자산명****(어플리케이션 포함)** | **수량** | **용도 및 주요기능** | **관리부서** | **ISMS와 중복수량** |
| *원격교육**서비스* | 서버 | *원격교육 웹서버* |  |  |  |  |
|  |  |  |  |  |
| 네트워크 |  |  |  |  |  |
| 보안장비 |  |  |  |  |  |
| 어플리케이션 | 관리자 페이지 |  |  |  |  |
| … |  |  |  |  |  |
| *공통인프라* |  |  |  |  |  |  |

o 시스템 및 네트워크 구성도

|  |
| --- |
| *☞ 신청기관의 전체 시스템 및 네트워크 구성도를 삽입하고, 생략 범위에 해당하는 영역 표시****(예시)***EMB00000d6007bb |

o 조직 범위

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **부서명(또는 용역업체명)** | **업 무** | **내부인력** | **외부인력****(용역포함)** | **ISMS와 중복인원** |
| *인사팀* | *인적보안 및 교육* | *xxx명* | xxx명 | xxx명 |
| *감사실* | *내부 보안감사* |  |  |  |
| *네트워크관리팀* | *네트워크 장비 및 보안장비 운영* |  |  |  |
| *…* | *…* |  |  |  |
| *…* | *…* |  |  |  |
| *…* | *…* |  |  |  |
| **합 계** | **xxx명** | **xxx명** | xxx명 |

o 조직도

|  |
| --- |
| *☞ 신청기관에서 인증 또는 정보보호 조치한 범위의 전체 조직도를 명시하고, 생략 범위에 해당하는 조직을 표시****(예시)*** EMB000005582652 |

**2. 인증심사 생략 항목 : 총 *OO*개**

※ 국제표준 정보보호 인증 또는 정보보호 조치 정보 중 1개 선택하여 작성

o 국제표준 정보보호경영시스템 인증

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **구분** | **항목** | **생략 신청** | **항목** | **생략 신청** |
| **국제표준 정보보호경영시스템 인증** | 1.1.1  | 정책의 승인 및 공표 |  | 7.3.1 | 개인업무 환경 보안 |  |
| 1.1.2 | 정책의 공표 |  | 7.3.2 | 공용업무 환경 보안 |  |
| 1.3.1  | 정책의 검토 |  | 8.1.1 | 보안 요구사항 정의 및 구현 |  |
| 1.3.2 | 정책문서 관리 |  | 8.1.2 | 인증 및 암호화 기능 |  |
| 2.2.1 | 역할 및 책임 |  | 8.1.3 | 보안로그 기능 |  |
| 3.1.1  | 외부자 계약 시 보안요구 사항 |  | 8.1.4 | 접근권한 기능 |  |
| 3.2.1  | 외부자 보안 이행 관리 |  | 8.3.1 | 외주개발보안 |  |
| 3.2.2 | 외부자 계약 만료 시 보안 |  | 9.1.1 | 암호 정책 수립 |  |
| 4.1.1 | 정보자산 식별 |  | 9.2.1 | 암호키 생성 및 이용 |  |
| 4.1.2 | 정보자산별 책임할당 |  | 10.1.1 | 접근통제 정책 수립 |  |
| 4.2.1 | 보안등급과 취급 |  | 12.1.1 | 침해사고 대응절차 수립 |  |
| 5.1.1 | 교육계획 |  | 12.1.2 | 침해사고 대응체계 구축 |  |
| 5.1.2 | 교육대상 |  | 11.4.1 | 정보시스템 저장매체 관리 |  |
| 5.1.3 | 교육내용 및 방법 |  | 11.4.2 | 휴대용 저장매체 관리 |  |
| 6.1.1  | 주요직무자 지정 및 감독 |  | 11.6.1 | 시각 동기화 |  |
| 6.1.2 | 직무 분리 |  | 11.6.2 | 로그기록 및 검토 |  |
| 6.1.3 | 정보보호 서약서 |  | 11.6.3 | 접근 및 사용 모니터링 |  |
| 6.2.1  | 퇴직 및 직무변경 관리 |  | 11.6.4 | 침해시도 모니터링 |  |
| 6.2.2 | 상벌규정 |  | 12.2.1 | 침해사고 훈련 |  |
| 7.1.1 | 보호구역지정 |  | 12.2.2 | 침해사고 보고 |  |
| 7.1.2 | 보호설비 |  | 12.2.3 | 침해사고 처리 및 복구 |  |
| 7.1.3 | 보호구역 내 작업 |  | 12.3.1 | 침해사고 분석 및 공유 |  |
| 7.1.4 | 출입통제 |  | 12.3.2 | 재발방지 |  |
| 7.1.5 | 모바일기기 반출입 |  | 13.1.1 | IT 재해복구 체계 구축 |  |
| 7.2.1 | 케이블 보안 |  | 13.2.1 | 영향분석에 따른 복구대책 수립 |  |
| 7.2.2 | 시스템 배치 및 관리 |  | 13.2.2 | 시험 및 유지관리 |  |
| 합계 | 개 |

o 개인정보보호 관리체계 인증

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **구분** | **항목** | **생략 신청** | **항목** | **생략 신청** |
| **개인정보보호 관리체계 인증** | 1.1.1  | 정책의 승인 및 공표 |  | 7.2.1 | 케이블 보안 |  |
| 1.1.2 | 정책의 공표 |  | 7.2.2 | 시스템 배치 및 관리 |  |
| 1.3.1  | 정책의 검토 |  | 7.3.1 | 개인업무 환경 보안 |  |
| 1.3.2 | 정책문서 관리 |  | 7.3.2 | 공용업무 환경 보안 |  |
| 2.1.1 | 정보보호 최고책인자 지정 |  | 9.1.1 | 암호 정책 수립 |  |
| 2.1.2 | 정보보호 실무조직 |  | 9.2.1 | 암호키 생성 및 이용 |  |
| 2.1.3 | 정보보호 위원회 |  | 10.1.1 | 접근통제 정책 수립 |  |
| 2.2.1 | 역할 및 책임 |  | 11.1.1 | 운영절차 수립 |  |
| 5.1.1 | 교육계획 |  | 11.4.1 | 정보시스템 저장매체 관리 |  |
| 5.1.2 | 교육대상 |  | 11.4.2 | 휴대용 저장매체 관리 |  |
| 5.1.3 | 교육내용 및 방법 |  | 11.6.1 | 시각 동기화 |  |
| 5.2.1 | 교육 시행 및 평가 |  | 11.6.2 | 로그기록 및 검토 |  |
| 6.1.1  | 주요직무자 지정 및 감독 |  | 11.6.3 | 접근 및 사용 모니터링 |  |
| 6.1.2 | 직무 분리 |  | 11.6.4 | 침해시도 모니터링 |  |
| 6.1.3 | 정보보호 서약서 |  | 12.1.1 | 침해사고 대응절차 수립 |  |
| 7.1.1 | 보호구역지정 |  | 12.1.2 | 침해사고 대응체계 구축 |  |
| 7.1.2 | 보호설비 |  | 12.2.1 | 침해사고 훈련 |  |
| 7.1.3 | 보호구역 내 작업 |  | 12.2.2 | 침해사고 보고 |  |
| 7.1.4 | 출입통제 |  | 12.2.3 | 침해사고 처리 및 복구 |  |
| 7.1.5 | 모바일기기 반출입 |  |  |  |  |
| 합계 | 개 |

o 「정보통신기반 보호법」제9조에 따른 취약점의 분석ㆍ평가

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **구분** | **항목** | **생략 신청** | **항목** | **생략 신청** |
| **「정보통신기반 보호법」제9조에 따른 취약점의 분석ㆍ평가** | 1.3.1  | 정책의 검토 |  | 7.1.2 | 보호설비 |  |
| 1.3.2 | 정책문서 관리 |  | 7.1.3 | 보호구역 내 작업 |  |
| 2.1.1 | 정보보호 최고책인자 지정 |  | 7.1.4 | 출입통제 |  |
| 2.1.2 | 정보보호 실무조직 |  | 7.1.5 | 모바일기기 반출입 |  |
| 2.1.3 | 정보보호 위원회 |  | 7.2.1 | 케이블 보안 |  |
| 3.1.1  | 외부자 계약 시 보안요구 사항 |  | 7.2.2 | 시스템 배치 및 관리 |  |
| 3.2.1  | 외부자 보안 이행 관리 |  | 8.2.1 | 구현 및 시험 |  |
| 3.2.2 | 외부자 계약 만료 시 보안 |  | 8.2.2 | 개발과 운영 환경 분리 |  |
| 4.1.1 | 정보자산 식별 |  | 8.2.3 | 운영환경 이관 |  |
| 4.1.2 | 정보자산별 책임할당 |  | 8.2.4 | 시험 데이터 보안 |  |
| 4.2.1 | 보안등급과 취급 |  | 8.2.5 | 소스 프로그램 보안 |  |
| 5.1.1 | 교육계획 |  | 10.1.1 | 접근통제 정책 수립 |  |
| 5.1.2 | 교육대상 |  | 10.3.1 | 사용자 인증 |  |
| 5.1.3 | 교육내용 및 방법 |  | 10.3.2 | 사용자 식별 |  |
| 6.1.1  | 주요직무자 지정 및 감독 |  | 10.3.3 | 사용자 패스워드 관리 |  |
| 6.1.2 | 직무 분리 |  | 12.1.1 | 침해사고 대응절차 수립 |  |
| 6.1.3 | 정보보호 서약서 |  | 12.1.2 | 침해사고 대응체계 구축 |  |
| 7.1.1 | 보호구역지정 |  |  |  |  |
| 합계 | 개 |

[별지1] 정보보호 관리체계 운영명세서 양식

**1. 정보보호관리과정**

|  |  |  |
| --- | --- | --- |
|  | **< 작성 時 주요 착안 사항 >** |  |
|  |  |
| 정보보호관리과정은 필수적인 항목으로 해당 인증기준을 모두 선택하여야 한다. 운영여부와 운영내용을 확인할 수 있도록 다음 항목을 상세히 작성하여야 한다. 항목별 설명은 다음과 같다.o 상세내용 : 신청기관 참고사항. 각 통제항목별로 의미하는 바를 기재하였음 (운영현황 등의 작성 공란이 부족할 경우 상세내용 삭제)o 수립여부 : 정보보호관리과정은 필수적으로 수립 및 구축해야 하므로 자가진단을 통해 Y/N으로 수립 및 구축을 확인o 운영현황 : **인증기준의 통제항목이 아닌 각 점검항목 수준으로 운영하고 있는 내용을 육하원칙으로 상세히 기재****※ 1개 통제항목에는 1개 이상의 점검항목이 존재**o 관련문서 : 인증기준을 만족하는 내용이 포함되어있는 기관의 문서 제목을 작성하되 문서 내 부분에 해당할 경우 장, 절, 조 등을 표시. 문서번호가 있다면 문서번호도 표시o 기록(증적자료) : 인증기준을 만족하는 내용이 포함되어있는 기관의 기록(증적자료) 제목 및 번호를 작성 |

| **통제항목** | **상세내용** | **수립****여부** | **운영현황** | **관련문서****(정책, 지침 등 세부조항번호까지)** | **기록(증적자료)** |
| --- | --- | --- | --- | --- | --- |
| **1. 정보보호정책수립 및 범위설정** |
| **1.1** | **정보보호정책의 수립** | 조직이 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호정책을 수립하고 동 정책은 국가나 관련 산업에서 정하는 정보보호 관련 법, 규제를 만족하여야 한다. | 　 |  | 　 | 　 |
| **1.2** | **범위설정** | 조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 정보보호 관리체계 범위를 설정하고 범위 내 모든 자산을 식별하여 문서화하여야 한다.  | 　 | 　 | 　 | 　 |
| **2. 경영진 책임 및 조직구성** |
| **2.1** | **경영진 참여** | 정보보호 관리체계 수립 및 운영 등 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여야 한다. | 　 | 　 | 　 | 　 |
| **2.2** | **정보보호 조직 구성 및 자원 할당** | 최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호 조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는데 필요한 자원(예산 및 인력)을 확보하여야 한다.  | 　 | 　 | 　 | 　 |
| **3. 위험관리** |
| **3.1** | **위험관리 방법 및 계획 수립** | 관리적, 기술적, 물리적, 법적 분야 등 조직의 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법을 선정하고 위험관리의 전문성을 보장할 수 있도록 수행인원, 기간, 대상, 방법 등을 구체적으로 포함한 위험관리계획을 사전에 수립하여야 한다. | 　 | 　 | 　 | 　 |
| **3.2** | **위험식별 및 평가** | 위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리하여야 한다.  | 　 | 　 | 　 | 　 |
| **3.3** | **정보보호대책 선정 및 이행계획 수립** | 위험을 수용 가능한 수준으로 감소시키기 위해 정보보호대책을 선정하고 그 보호대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다. | 　 | 　 | 　 | 　 |
| **4. 정보보호대책 구현** |
| **4.1** | **정보보호대책의 효과적 구현** | 정보보호대책 이행계획에 따라 보호대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다. | 　 | 　 | 　 | 　 |
| **4.2** | **내부 공유 및 교육** | 구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다. | 　 | 　 | 　 | 　 |
| **5 사후관리** |
| **5.1** | **법적요구사항 준수검토** | 조직이 준수해야 할 정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다. | 　 | 　 | 　 | 　 |
| **5.2** | **정보보호 관리체계 운영현황 관리** | 정보보호 관리체계 범위 내에서 주기적 또는 상시적으로 수행해야 하는 활동을 문서화하고 그 운영현황을 지속적으로 관리하여야 한다. | 　 | 　 | 　 | 　 |
| **5.3** | **내부감사** | 조직은 정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는 지를 점검하기 위하여 연 1회 이상 내부감사를 수행하여야 한다. 이를 위해 감사 기준, 범위, 주기, 방법 등을 구체적으로 정하고 내부감사를 통해 발견된 문제점은 보완조치를 완료하여 경영진 및 관련 책임자에게 보고하여야 한다. 또한 감사의 독립성 및 전문성을 확보할 수 있도록 감사인력에 대한 자격요건을 정의하여야 한다. | 　 | 　 | 　 | 　 |

**2. 정보보호대책**

|  |  |  |
| --- | --- | --- |
|  | **< 작성 時 주요 착안 사항 >** |  |
|  |  |
| 정보보호 대책은 기업의 정보보호 운영현황에 따라 선택할 수 있다. 선택하지 않은 통제항목의 경우 미선택 사유를 작성하여야 한다. 선택한 경우에는 선택이유 및 구현내용을 확인할 수 있도록 선택사유, 적용내용, 관련문서, 기록(증적자료)을 상세히 작성하여야 한다.o 상세내용 : 신청기관 참고사항. 각 통제항목별로 의미하는 바를 기재하였음 (운영현황 등의 작성 공란이 부족할 경우 상세내용 삭제)o 선택여부 : 정보보호 대책의 선택여부에 대해 Y(Yes) / N(No)로 표시 **(N은 해당통제사항이 기업의 운영환경 상 적용되지 않는 경우에 기재)**o 운영현황(또는 미선택사유) : **인증기준의 통제항목이 아닌 각 점검항목 수준으로 운영하고 있는 내용을 육하원칙으로 상세히 기재****※ 1개 통제항목에는 1개 이상의 점검항목이 존재**해당 통제사항에 대한 구축 및 실제 운영내용을 요약하여 작성하되 구축의 특성 및 정당성을 파악할 수 있도록 인증기준보다 상세히 작성. 통제사항을 선택하지 않은 경우 위험관리(위험평가 및 처리)의 결과 및 분석에 따른 미선택의 사유를 반드시 작성.o 관련문서(정책 또는 매뉴얼) : 인증기준을 만족하는 내용이 포함되어있는 기관의 문서(정책, 규정, 지침, 절차, 매뉴얼 등)의 제목을 작성하되 문서 내 부분에 해당할 경우 장, 절, 조 등을 상세하게 표시. 선택하지 않을 경우, 해당 근거를 확인할 수 있는 문서 및 문서 내 부분을 작성. 문서번호가 있다면 문서번호도 표시.o 기록(증적자료) : 인증기준을 만족하는 내용이 포함되어있는 기관의 운영기록(증적자료)의 제목(파일명) 및 번호를 작성. 통제사항에 관련된 위험분석결과, 계획, 취약점분석관련 자료도 기록하여 운영명세서를 통해 관련내용을 확인할 수 있도록 함. 관련증적이 시스템으로 관리되는 경우 해당 시스템 위치, 시스템명 및 관련 메뉴를 작성. |

| **통제항목** | **상세내용** | **선택****여부** | **운영현황****(또는 미선택사유)** | **관련문서****(정책, 지침 등 세부조항번호까지)** | **기록(증적자료)** |
| --- | --- | --- | --- | --- | --- |
| **1. 정보보호 정책**  |
| **1.1 정책의 승인 및 공표** |
| **1.1.1** | **정책의 승인** | 정보보호정책은 이해관련자의 검토와 최고경영자의 승인을 받아야 한다. |  |  |  |  |
| **1.1.2** | **정책의 공표** | 정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다. |  |  |  |  |
| **1.2 정책의 체계** |
| **1.2.1** | **상위 정책과의 연계성** | 정보보호정책은 상위조직 및 관련 기관의 정책과 연계성을 유지하여야 한다. |  |  |  |  |
| **1.2.2** | **정책시행 문서수립** | 정보보호정책의 구체적인 시행을 위한 정보보호지침, 절차를 수립하고 관련 문서간의 일관성을 유지하여야 한다. |  |  |  |  |
| **1.3 정책의 유지관리** |
| **1.3.1** | **정책의 검토** | 정기적으로 정보보호정책 및 정책 시행문서의 타당성을 검토하고, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발견, 정보보호 환경에 중대한 변화 등이 정보보호정책에 미치는 영향을 분석하여 필요한 경우 제･개정하여야 한다. |  |  |  |  |
| **1.3.2** | **정책문서 관리** | 정보보호정책 및 정책 시행문서의 이력관리를 위해 제정, 개정, 배포, 폐기 등의 관리절차를 수립하고 문서는 최신본으로 유지하여야 한다. 또한 정책문서 시행에 따른 운영기록을 생성하여 유지하여야 한다.  |  |  |  |  |
| **2. 정보보호 조직**  |
| **2.1 조직 체계** |
| **2.1.1** | **정보보호 최고 책임자  지정** | 최고경영자는 임원급의 정보보호 최고책임자를 지정하고 정보보호 최고책임자는 정보보호정책 수립, 정보보호 조직 구성, 위험관리, 정보보호위원회 운영 등의 정보보호에 관한 업무를 총괄 관리하여야 한다. |  |  |  |  |
| **2.1.2** | **실무조직 구성** | 최고경영자는 정보보호 최고책임자의 역할을 지원하고 조직의 정보보호활동을 체계적으로 이행하기 위해 실무조직을 구성하고 조직 구성원의 정보보호 전문성을 고려하여 구성한다.  |  |  |  |  |
| **2.1.3** | **정보보호****위원회** | 정보보호 자원할당 등 조직 전반에 걸친 중요한 정보보호 관련사항에 대한 검토 및 의사결정을 할 수 있도록 정보보호위원회를 구성하여 운영하여야 한다. |  |  |  |  |
| **2.2 역할 및 책임** |
| **2.2.1** | **역할 및 책임** | 정보보호 최고책임자와 정보보호 관련 담당자에 대한 역할 및 책임을 정의하고 그 활동을 평가할 수 있는 체계를 마련하여야 한다.  |  |  |  |  |
| **3. 외부자 보안**  |
| **3.1 보안 요구사항 정의** |
| **3.1.1** | **외부자 계약 시 보안요구사항** | 조직의 정보처리 업무를 외부자에게 위탁하거나 정보자산에 대한 접근을 허용할 경우, 또는 업무를 위해 클라우드 서비스 등 외부 서비스를 이용하는 경우에는 보안요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시하여야 한다. |  |  |  |  |
| **3.2 외부자 보안 이행** |
| **3.2.1** | **외부자 보안 이행 관리** | 외부자가 계약서 및 협정서에 명시된 보안요구사항의 이행여부를 관리 감독하고 주기적인 점검 또는 감사를 수행하여야 한다.  |  |  |  |  |
| **3.2.2** | **외부자 계약 만료 시 보안** | 외부자와의 계약만료, 업무종료, 담당자변경 시 조직이 외부자에게 제공한 정보자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 시 알게 된 정보의 비밀유지확약서 등의 내용을 확인하여야 한다. |  |  |  |  |
| **4 정보자산 분류** |
| **4.1 정보자산 식별 및 책임**  |
| **4.1.1** | **정보자산 식별** | 조직의 업무특성에 따라 정보자산 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별하여야 한다. 또한 식별된 정보자산을 목록으로 관리하여야 한다. |  |  |  |  |
| **4.1.2** | **정보자산별 책임할당** | 식별된 정보자산에 대한 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다. |  |  |  |  |
| **4.2 정보자산의 분류 및 취급** |
| **4.2.1** | **보안등급과 취급** | 기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산이 조직에 미치는 중요도를 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다. 또한 보안등급을 표시하고 등급 부여에 따른 취급절차를 정의하여 이행하여야 한다. |  |  |  |  |
| **5. 정보보호 교육**  |
| **5.1 교육 프로그램 수립** |
| **5.1.1** | **교육계획** | 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호교육 계획을 수립하여야 한다. |  |  |  |  |
| **5.1.2** | **교육대상** | 교육 대상에는 정보보호 관리체계 범위 내 임직원 및 외부자를 모두 포함하여야 한다. |  |  |  |  |
| **5.1.3** | **교육내용 및 방법** | 교육에는 정보보호 및 정보보호 관리체계 개요, 보안사고 사례, 내부 규정 및 절차, 법적 책임 등의 내용을 포함하고 일반 임직원, 책임자, IT 및 정보보호 담당자 등 각 직무별 전문성 제고에 적합한 교육내용 및 방법을 정하여야 한다. |  |  |  |  |
| **5.2 교육 시행 및 평가** |
| **5.2.1** | **교육 시행 및 평가** | 정보보호 관리체계 범위 내 임직원 및 외부자를 대상으로 연 1회 이상 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 조직 내․외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생할 경우 추가 교육을 수행하여야 한다. 또한 교육 시행에 대한 기록을 남기고 평가하여야 한다. |  |  |  |  |
| **6 인적 보안**  |
| **6.1 정보보호 책임** |
| **6.1.1** | **주요 직무자 지정 및 감독** | 인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급하는 임직원의 경우 주요직무자로 지정하고 주요직무자 지정을 최소화 하는 등 관리할 수 있는 보호대책을 수립하여야 한다.  |  |  |  |  |
| **6.1.2** | **직무 분리** | 권한 오남용 등 고의적인 행위로 인해 발생할 수 있는 잠재적인 피해를 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 인적자원 부족 등 불가피하게 직무분리가 어려운 경우 별도의 보완통제를 마련하여야 한다. |  |  |  |  |
| **6.1.3** | **비밀유지서약서** | 임직원으로부터 비밀유지 서약서를 받아야 하고 임시직원이나 외부자에게 정보시스템에 대한 접근권한을 부여할 경우에도 비밀유지서약서를 받아야 한다. |  |  |  |  |
| **6.2 인사규정** |
| **6.2.1** | **퇴직 및 직무변경 관리** | 퇴직 및 직무변경 시 인사부서와 정보보호 및 시스템 운영 부서 등 관련 부서에서 이행해야 할 자산반납, 접근권한 회수․조정, 결과 확인 등의 절차를 수립하여야 한다. |  |  |  |  |
| **6.2.2** | **상벌규정** | 인사규정에 직원이 정보보호 책임과 의무를 충실히 이행했는지 여부 등 정보보호 활동 수행에 따른 상벌 규정을 포함하여야 한다. |  |  |  |  |
| **7 물리적 보안**  |
| **7.1 물리적 보호구역** |
| **7.1.1** | **보호구역지정** | 비인가자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 주요 설비 및 시스템을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립․이행하여야 한다.  |  |  |  |  |
| **7.1.2** | **보호설비** | 각 보호구역의 중요도 및 특성에 따라 화재, 전력이상 등 인․재해에 대비하여 온습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 설비를 충분히 갖추고 운영절차를 수립하여 운영하여야 한다. 또한 주요 시스템을 외부 집적정보통신시설에 위탁운영하는 경우 관련 요구사항을 계약서에 반영하고 주기적으로 검토를 수행하여야 한다. |  |  |  |  |
| **7.1.3** | **보호구역 내 작업** | 유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.  |  |  |  |  |
| **7.1.4** | **출입통제** | 보호구역 및 보호구역 내 주요 설비 및 시스템은 인가된 사람만이 접근할 수 있도록 출입을 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다. |  |  |  |  |
| **7.1.5** | **모바일 기기 반출입** | 노트북 등 모바일 기기 미승인 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부자 모바일 기기 반출입 통제절차를 수립하고 기록․관리하여야 한다.  |  |  |  |  |
| **7.2 시스템 보호** |
| **7.2.1** | **케이블 보안** | 데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상을 입지 않도록 보호하여야 한다. |  |  |  |  |
| **7.2.2** | **시스템 배치 및 관리** | 시스템은 그 특성에 따라 분리하여 배치하고 장애 또는 보안사고 발생 시 주요 시스템의 위치를 즉시 확인할 수 있는 체계를 수립하여야 한다. |  |  |  |  |
| **7.3 사무실 보안** |
| **7.3.1** | **개인업무 환경 보안** | 일정시간 동안 자리를 비울 경우에는 책상 위에 중요한 문서나 저장매체를 남겨놓지 않고 컴퓨터 화면에 중요정보가 노출되지 않도록 화면보호기 설정, 패스워드 노출 금지 등 보호대책을 수립하여야 한다. |  |  |  |  |
| **7.3.2** | **공용업무 환경 보안** | 사무실에서 공용으로 사용하는 사무처리 기기, 문서고, 공용 PC, 파일서버 등을 통해 중요정보 유출이 발생하지 않도록 보호대책을 마련하여야 한다. |  |  |  |  |
| **8. 시스템 개발보안**  |
| **8.1 분석 및 설계 보안관리** |
| **8.1.1** | **보안 요구사항 정의** | 신규 정보시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다. |  |  |  |  |
| **8.1.2** | **인증 및 암호화 기능** | 정보시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입․출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다. |  |  |  |  |
| **8.1.3** | **보안로그 기능** | 정보시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다. |  |  |  |  |
| **8.1.4** | **접근권한 기능** | 정보시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다. |  |  |  |  |
| **8.2 구현 및 이관 보안** |
| **8.2.1** | **구현 및 시험** | 안전한 코딩방법에 따라 정보시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다. 또한 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다. |  |  |  |  |
| **8.2.2** | **개발과 운영 환경 분리** | 개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.  |  |  |  |  |
| **8.2.3** | **운영환경 이관** | 운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고 실행코드는 시험과 사용자 인수 후 실행하여야 한다.  |  |  |  |  |
| **8.2.4** | **시험데이터 보안** | 시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다. |  |  |  |  |
| **8.2.5** | **소스 프로그램 보안** | 소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다. |  |  |  |  |
| **8.3 외주개발보안** |
| **8.3.1** | **외주개발보안** | 정보시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리․감독하여야 한다. |  |  |  |  |
| **9 암호통제**  |
| **9.1 암호 정책** |
| **9.1.1** | **암호 정책 수립** | 조직의 중요정보 보호를 위하여 암호화 대상, 암호 강도(복잡도), 키관리, 암호사용에 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다. |  |  |  |  |
| **9.2 암호키 관리** |
| **9.2.1** | **암호키 생성 및 이용** | 암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 필요 시 복구방안을 마련하여야 한다. |  |  |  |  |
| **10. 접근통제**  |
| **10.1 접근통제 정책** |
| **10.1.1** | **접근통제 정책 수립** | 비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다. |  |  |  |  |
| **10.2 접근권한 관리** |
| **10.2.1** | **사용자 등록 및 권한부여** | 정보시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다. |  |  |  |  |
| **10.2.2** | **관리자 및 특수 권한 관리** | 정보시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.  |  |  |  |  |
| **10.2.3** | **접근권한 검토** | 정보시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.  |  |  |  |  |
| **10.3 사용자 인증 및 식별** |
| **10.3.1** | **사용자 인증** | 정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제되어야 하고. 필요한 경우 법적요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다. |  |  |  |  |
| **10.3.2** | **사용자 식별** | 정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.  |  |  |  |  |
| **10.3.3** | **사용자 패스워드 관리** | 법적요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립․이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.  |  |  |  |  |
| **10.3.4** | **이용자 패스워드 관리** | 고객, 회원 등 외부 이용자가 접근하는 정보시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다. |  |  |  |  |
| **10.4 접근통제 영역** |
| **10.4.1** | **네트워크 접근** | 네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내･외부 네트워크를 분리하여야 한다.  |  |  |  |  |
| **10.4.2** | **서버 접근** | 서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다. |  |  |  |  |
| **10.4.3** | **응용 프로그램 접근** | 사용자의 업무 또는 직무에 따라 응용프로그램 접근권한을 제한하고 불필요한 중요정보 노출을 최소화해야 한다. |  |  |  |  |
| **10.4.4** | **데이터베이스 접근** | 데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립하여야 한다. 또한 중요정보를 저장하고 있는 데이터베이스의 경우 사용자 접근내역을 기록하고 접근의 타당성을 정기적으로 검토하여야 한다. |  |  |  |  |
| **10.4.5** | **모바일 기기 접근** | 모바일기기를 업무 목적으로 내․외부 네트워크에 연결하여 활용하는 경우 중요정보 유출 및 침해사고 예방을 위해 기기 인증 및 승인, 접근 범위, 기기 보안설정, 오남용 모니터링 등의 접근통제 대책을 수립하여야 한다.  |  |  |  |  |
| **10.4.6** | **인터넷 접속** | 인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급․운영하는 주요직무자의 경우 인터넷 접속 또는 서비스(P2P, 웹메일, 웹하드, 메신저 등)를 제한하고 인터넷 접속은 침입차단시스템을 통해 통제하여야 한다. 필요시 침입탐지시스템 등을 통해 인터넷 접속내역을 모니터링하여야 한다. |  |  |  |  |
| **11 운영보안**  |
| **11.1 운영절차 및 변경관리**  |
| **11.1.1** | **운영절차 수립** | 정보시스템 동작, 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다. |  |  |  |  |
| **11.1.2** | **변경관리** | 정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립하고 변경 전 시스템의 전반적인 성능 및 보안에 미치는 영향을 분석하여야 한다. |  |  |  |  |
| **11.2 시스템 및 서비스 운영보안** |
| **11.2.1** | **정보시스템 인수** | 새로운 정보시스템 도입 또는 개선 시 필수 보안요구사항을 포함한 인수 기준을 수립하고 인수 전 기준 적합성을 검토하여야 한다. |  |  |  |  |
| **11.2.2** | **보안시스템 운영** | 보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템 별 정책적용 현황을 관리하여야 한다. |  |  |  |  |
| **11.2.3** | **성능 및 용량관리** | 정보시스템 및 서비스 가용성 보장을 위해 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링할 수 있는 방법 및 절차를 수립하여야 한다. |  |  |  |  |
| **11.2.4** | **장애관리** | 정보시스템 장애 발생 시 효과적으로 대응하기 위한 탐지, 기록, 분석, 복구, 보고 등의 절차를 수립하여야 한다.  |  |  |  |  |
| **11.2.5** | **원격운영관리** | 내부 네트워크를 통하여 정보시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 원칙적으로 금지하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등의 보호대책을 수립하여야 한다. |  |  |  |  |
| **11.2.6** | **스마트워크 보안** | 재택근무, 원격협업 등과 같은 원격 업무 수행 시 이에 대한 관리적․기술적 보호대책을 수립하고 이행하여야 한다.  |  |  |  |  |
| **11.2.7** | **무선네트워크 보안** | 무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.  |  |  |  |  |
| **11.2.8** | **공개서버 보안** | 웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다. |  |  |  |  |
| **11.2.9** | **백업관리** | 데이터의 무결성 및 정보시스템의 가용성을 유지하기 위해 백업 대상, 주기, 방법 등의 절차를 수립하고 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다. |  |  |  |  |
| **11.2.10** | **취약점 점검** | 정보시스템이 알려진 취약점에 노출되어 있는 지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.  |  |  |  |  |
| **11.3 전자거래 및 정보전송 보안** |
| **11.3.1** | **전자거래 보안** | 전자거래 서비스 제공 시 정보유출, 데이터 조작, 사기 등의 침해사고를 예방하기 위해 사용자 인증, 암호화, 부인방지 등의 보호대책을 수립하고 결제시스템 등 외부 시스템과의 연계가 필요한 경우 연계 안전성을 점검하여야 한다. |  |  |  |  |
| **11.3.2** | **정보전송 정책 수립 및 협약 체결** | 타 조직에 중요정보를 전송할 경우 안전한 전송을 위한 정책을 수립하고 조직 간 정보전송 합의를 통해 관리 책임, 전송 기술 표준, 중요정보의 보호를 위한 기술적 보호조치 등을 포함한 협약서를 작성하여야 한다. |  |  |  |  |
| **11.4 매체 보안** |
| **11.4.1** | **정보시스템 저장매체 관리** | 정보시스템 폐기 또는 재사용 시 중요정보를 담고 있는 하드디스크, 스토리지, 테잎 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다. |  |  |  |  |
| **11.4.2** | **휴대용 저장매체 관리** | 조직의 중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.  |  |  |  |  |
| **11.5 악성코드 관리** |
| **11.5.1** | **악성코드 통제** | 바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립하여야 한다. |  |  |  |  |
| **11.5.2** | **패치관리** | 소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인해 발생할 수 있는 침해사고를 예방하기 위해 최신 패치를 정기적으로 적용하고 필요한 경우 시스템에 미치는 영향을 분석하여야 한다. |  |  |  |  |
| **11.6 로그관리 및 모니터링** |
| **11.6.1** | **시각동기화** | 로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 정보시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다. |  |  |  |  |
| **11.6.2** | **로그기록 및 보존** | 정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그유형을 정의하여 일정기간 보존하고 주기적으로 검토하여야 한다. 보존기간 및 검토주기는 법적요구사항을 고려하여야 한다. |  |  |  |  |
| **11.6.3** | **접근 및 사용 모니터링** | 중요정보, 정보시스템, 응용프로그램, 네트워크 장비에 대한 사용자 접근이 업무상 허용된 범위에 있는 지 주기적으로 확인하여야 한다. |  |  |  |  |
| **11.6.4** | **침해시도 모니터링** | 외부로부터의 침해시도를 모니터링 하기 위한 체계 및 절차를 수립하여야 한다.  |  |  |  |  |
| **12. 침해사고 관리**  |
| **12.1 절차 및 체계** |
| **12.1.1** | **침해사고대응절차 수립** | DDoS 등 침해사고 유형별 중요도 분류, 유형별 보고․대응․복구 절차, 비상연락체계, 훈련 시나리오 등을 포함한 침해사고 대응 절차를 수립하여야 한다. |  |  |  |  |
| **12.1.2** | **침해사고 대응체계 구축** | 침해사고 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고 외부기관 및 전문가들과의 협조체계를 수립하여야 한다. |  |  |  |  |
| **12.2 대응 및 복구** |
| **12.2.1** | **침해사고 훈련** | 침해사고 대응 절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다. |  |  |  |  |
| **12.2.2** | **침해사고 보고** | 침해사고 징후 또는 사고 발생을 인지한 때에는 침해사고 유형별 보고절차에 따라 신속히 보고하고 법적 통지 및 신고 의무를 준수하여야 한다.  |  |  |  |  |
| **12.2.3** | **침해사고 처리 및 복구** | 침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다. |  |  |  |  |
| **12.3 사후관리** |
| **12.3.1** | **침해사고 분석 및 공유** | 침해사고가 처리되고 종결된 후 이에 대한 분석을 수행하고 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약점들을 관련 조직 및 임직원들과 공유하여야 한다. |  |  |  |  |
| **12.3.2** | **재발방지** | 침해사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하고 이를 위해 필요한 경우 정책, 절차, 조직 등의 대응체계를 변경하여야 한다. |  |  |  |  |
| **13. IT 재해복구**  |
| **13.1 체계 구축** |
| **13.1.1** | **IT 재해복구 체계 구축** | 자연재앙, 해킹, 통신장애, 전력중단 등의 요인으로 인해 IT 시스템 중단 또는 파손 등 피해가 발생할 경우를 대비하여 비상 시 복구조직, 비상연락체계, 복구절차 등 IT 재해복구 체계를 구축하여야 한다. |  |  |  |  |
| **13.2 대책 구현** |
| **13.2.1** | **영향분석에 따른 복구대책 수립** | 조직의 핵심 서비스 연속성을 위협할 수 있는 IT 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 IT 서비스 및 시스템 복구목표시간, 복구시점을 정의하고 적절한 복구전략 및 대책을 수립․이행하여야 한다. |  |  |  |  |
| **13.2.2** | **시험 및 유지관리** | IT 서비스 복구전략 및 대책에 따라 효과적인 복구가 가능한 지 시험을 실시하고 시험계획에는 시나리오, 일정, 방법, 절차 등을 포함하여야 한다. 또한 시험결과, IT 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.  |  |  |  |  |