DOC-POL-002

**정보보호 및 개인정보보호**

**업무지침**

개정번호 : 1.00

**㈜1 Shop**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **개 정 이 력** | | | | | | |
| **문서명** | | 정보보호 및 개인정보보호 업무지침 | | | | |
| **생성일** | | 2018.10.01 | **보안등급** | | 대외비 | |
| **소유자** | | ㈜1 Shop | **사용자(범위)** | |  | |
| **차수** | **Version** | **개정내용** | | **개정일자** | | **작성자** |
| 1 | 1.00 | 최초 작성 | | 2018.10.01 | | 최유진 |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |
|  |  |  | |  | |  |

**목 차**

[**제1장** **개요 8**](#_Toc381279730)

[제1조 목적 8](#_Toc381279731)

[제2조 적용대상 8](#_Toc381279732)

[**제2장** **정보보호정책 및 개인정보보호정책 관리 8**](#_Toc381279733)

[제3조 정보보호 및 개인정보보호 정책 및 지침의 문서화 8](#_Toc381279734)

[제4조 정보보호 및 개인정보보호 정책 및 지침의 평가 및 검토·변경 9](#_Toc381279735)

[제5조 이행점검 10](#_Toc381279736)

[**제3장** **정보보호조직 및 개인정보보호조직 관리 10**](#_Toc381279737)

[제6조 조직체계 10](#_Toc381279738)

[**제1절** **정보보호 주관부서 11**](#_Toc381279739)

[제7조 정보보호 최고책임자 11](#_Toc381279740)

[제8조 정보보호 관리자 12](#_Toc381279741)

[제9조 정보보호 담당자 13](#_Toc381279742)

[**제2절** **개인정보보호 주관부서 14**](#_Toc381279743)

[제10조 개인정보 관리책임자 14](#_Toc381279744)

[제11조 개인정보 관리자 14](#_Toc381279745)

[제12조 개인정보 담당자 15](#_Toc381279746)

[제13조 물리보안 담당자 16](#_Toc381279747)

[제14조 기술보안 담당자 17](#_Toc381279748)

[제15조 구성 18](#_Toc381279749)

[제16조 임무 18](#_Toc381279750)

[제17조 운영 19](#_Toc381279751)

[**제3절** **보안사고 대응반 20**](#_Toc381279752)

[제18조 구성 20](#_Toc381279753)

[제19조 임무 21](#_Toc381279754)

[제20조 운영 21](#_Toc381279755)

[**제4장** **정보자산 위험관리 21**](#_Toc381279756)

[**제1절** **정보자산 및 개인정보자산관리 21**](#_Toc381279757)

[제21조 자산의 식별 및 분류 21](#_Toc381279758)

[제22조 정보자산목록 작성 및 유지 22](#_Toc381279759)

[제23조 정보자산 가치평가 22](#_Toc381279760)

[제24조 정보시스템 목록 작성 및 유지 23](#_Toc381279761)

[제25조 문서 분류 23](#_Toc381279762)

[제26조 문서 관리 24](#_Toc381279763)

[제27조 저장매체 관리 24](#_Toc381279764)

[**제2절** **위협의 식별 및 평가 25**](#_Toc381279765)

[제28조 위협의 식별 25](#_Toc381279766)

[제29조 위협의 빈도 평가 25](#_Toc381279767)

[**제3절** **취약성 진단 및 평가 25**](#_Toc381279768)

[제30조 취약성 진단 25](#_Toc381279769)

[제31조 취약성 진단 결과의 유지 및 활용 26](#_Toc381279770)

[**제4절** **위험분석 26**](#_Toc381279771)

[제32조 위험도 측정 26](#_Toc381279772)

[제33조 허용가능 위험도의 결정 27](#_Toc381279773)

[**제5절** **보호대책 수립 및 이행 27**](#_Toc381279774)

[제34조 보호대책의 수립 및 공표 27](#_Toc381279775)

[제35조 보호대책의 이행 27](#_Toc381279776)

[**제6절** **사후관리 28**](#_Toc381279777)

[제36조 관리체계의 재검토 28](#_Toc381279778)

[제37조 관리체계의 모니터링 및 개선 28](#_Toc381279779)

[제38조 위험관리전략 및 계획수립 29](#_Toc381279780)

[**제5장** **생활환경보안 29**](#_Toc381279781)

[**제1절** **업무환경보안 29**](#_Toc381279782)

[제39조 개인정보 환경보안 29](#_Toc381279783)

[제40조 공용업무 환경보안 30](#_Toc381279784)

[**제2절** **물리적 보안 30**](#_Toc381279785)

[제41조 보호구역의 지정 30](#_Toc381279786)

[제42조 제한구역의 통제 31](#_Toc381279787)

[제43조 휴대용 전산장비의 반/출입 31](#_Toc381279788)

[제44조 영상정보 보안 32](#_Toc381279789)

[제45조 케이블 보안 32](#_Toc381279790)

[제46조 전원관리 32](#_Toc381279791)

[**제3절** **인력보안 32**](#_Toc381279792)

[제47조 주요직무자의 지정 33](#_Toc381279793)

[제48조 입퇴사 관리 33](#_Toc381279794)

[**제4절** **교육훈련 33**](#_Toc381279795)

[제49조 정보보호 교육계획의 수립 33](#_Toc381279796)

[제50조 교육대상 34](#_Toc381279797)

[제51조 교육의 시행 34](#_Toc381279798)

[**제6장** **개발 및 IT 인프라 운영보안 관리 35**](#_Toc381279799)

[**제1절** **개발 및 운영 관리 35**](#_Toc381279800)

[제52조 직무분리 35](#_Toc381279801)

[제53조 개발 관리 35](#_Toc381279802)

[제54조 IT 인프라 보안 관리 36](#_Toc381279803)

[**제2절** **정보처리시스템 및 개인정보처리시스템 관리 37**](#_Toc381279804)

[제55조 접근통제 37](#_Toc381279805)

[제56조 이동 컴퓨터 및 원격작업 38](#_Toc381279806)

[제57조 보안성 심의 38](#_Toc381279807)

[제58조 접속기록의 관리 40](#_Toc381279808)

[제59조 제3자 서비스 수행관리 40](#_Toc381279809)

[제60조 성능 및 용량관리 40](#_Toc381279810)

[제61조 장애관리 41](#_Toc381279811)

[**제3절** **암호화 41**](#_Toc381279812)

[제62조 암호화 대상 41](#_Toc381279813)

[제63조 암호화 적용 42](#_Toc381279814)

[제64조 안전한 키 관리 42](#_Toc381279815)

[**제7장** **개인정보보호관리 43**](#_Toc381279816)

[**제1절** **개인정보 관리 43**](#_Toc381279817)

[제65조 개인정보 관리계획(내부관리계획) 수립 및 이행 43](#_Toc381279818)

[제66조 개인정보의 식별 및 취급자의 지정 44](#_Toc381279819)

[제67조 개인정보 처리 방침의 작성 및 관리 44](#_Toc381279820)

[**제2절** **개인정보 수집관리 45**](#_Toc381279821)

[제68조 개인정보의 수집 및 동의 45](#_Toc381279822)

[제69조 수집시 최소화의 원칙 45](#_Toc381279823)

[제70조 중요정보의 수집제한 45](#_Toc381279824)

[제71조 고유식별정보의 수집제한 46](#_Toc381279825)

[제72조 개인정보 수집시 고지 46](#_Toc381279826)

[제73조 동의를 받는 방법 46](#_Toc381279827)

[**제3절** **개인정보 이용 관리 46**](#_Toc381279828)

[제74조 개인정보 이용의 제한 46](#_Toc381279829)

[제75조 개인정보의 위탁 47](#_Toc381279830)

[제76조 개인정보의 제3자 제공 47](#_Toc381279831)

[제77조 개인정보 위탁시 보안요구사항 48](#_Toc381279832)

[제78조 개인정보의 관리감독 48](#_Toc381279833)

[**제4절** **개인정보 파기 관리 48**](#_Toc381279834)

[제79조 파기 시점 48](#_Toc381279835)

[제80조 개인정보 파기 방법 49](#_Toc381279836)

[제81조 휴면 이용자 정보 파기 49](#_Toc381279837)

[**제5절** **정보주체의 권리 보호 49**](#_Toc381279838)

[제82조 개인정보의 열람 49](#_Toc381279839)

[제83조 동의의 철회 50](#_Toc381279840)

[제84조 개인정보 이용내역의 통지 50](#_Toc381279841)

[제85조 개인정보 유출 시 신고 50](#_Toc381279842)

[제86조 개인정보의 안전성 확보조치 51](#_Toc381279843)

[**제6절** **영상정보관리 51**](#_Toc381279844)

[제87조 영상정보관리 51](#_Toc381279845)

[**제8장** **감사 52**](#_Toc381279846)

[제88조 계획 수립 52](#_Toc381279847)

[제89조 조직 52](#_Toc381279848)

[제90조 방법 53](#_Toc381279849)

[제91조 사후 관리 53](#_Toc381279850)

[**제9장** **사고관리 53**](#_Toc381279851)

[제92조 보안사고 예방 활동 53](#_Toc381279852)

[제93조 보안사고 대응관리 53](#_Toc381279853)

[제94조 보안사고 결과보고 및 복구 54](#_Toc381279854)

[제95조 사후 관리 54](#_Toc381279855)

1. **개요**
2. **목적**

본 지침의 목적은 ㈜1 Shop(이하 ‘회사’라 한다.)의 정보에 대한 오남용, 훼손, 변조, 유출 등 정보보호 위협으로부터 서비스 및 중요 정보자산, 개인정보를 보호하기 위한 정보보호 업무를 규정함에 있다.

1. **적용대상**

정보보호의 적용 범위는 회사의 정보자산으로 한다. 정보자산은 정보, 정보시스템과 개인정보로 구분하며, 이를 운영하기 위하여 필요한 관련 자산 역시 정보보호의 대상이 되며 이에 대한 정의는 다음과 같다.

1. 정보의 범위는 임직원들이 경영활동과 관련하여 생성 또는 입수하여 소유하고 있는 아이디어, 지적 자산 등의 정보로서, 컴퓨터나 저장매체에 기록된 전자 정보와 인쇄물을 포함한다.
2. 정보시스템의 범위는 임직원이 사용 또는 관리하는 모든 하드웨어, 소프트웨어, 네트워크 등을 포함한다.
3. 개인정보는 전자적 처리 여부를 불문하고 수기문서, 개인영상정보를 포함한 모든 형태의 개인정보를 말한다.
4. 관련 자산은 정보 및 정보시스템에 관련된 인력, 시설, 장비 및 운영을 위한 문서 등을 포함한다.
5. **정보보호정책 및 개인정보보호정책 관리**
6. **정보보호 및 개인정보보호 정책 및 지침의 문서화**
7. 본 정보보호, 개인정보 주관부서는 정보보호 및 개인정보보호 정책, 지침을 문서화한다.
8. 수립된 정보보호 및 개인정보보호 정책서는 최고경영자의 승인 후 시행하며 정보보호 및 개인정보보호 업무 지침은 정보보호 최고책임자의 승인 후 시행한다.
9. 승인을 득한 정보보호 및 개인정보보호 정책, 지침은 정보보호 관리자가 회람, 게시 등 적절한 방법을 통하여 전 임직원 및 관계된 모든 인원들이 인식할 수 있도록 공표한다.
10. 회사의 임직원 및 관련 인력들은 문서화된 정보보호 및 개인정보보호 정책, 지침을 준수하여 업무를 수행하여야 한다.
11. 정보보호 및 개인정보보호 정책, 지침 문서는 “문서관리 절차서”에 따라 목적, 적용범위, 책임 및 권한, 세부 업무절차 등을 명시하여야 하며 개정이력을 관리하여야 한다.
12. **정보보호 및 개인정보보호 정책 및 지침의 평가 및 검토·변경**
13. 정보보호, 개인정보보호 주관부서는 정보보호 및 개인정보보호 정책, 지침에 대하여 연 1회 다음 사항을 검토하고 평가하여야 한다.
14. 정보보호 정책 및 지침의 효과성
15. 사업 효율성 측면에서의 통제 비용과 영향
16. 기술 변화 및 보안 사고 발생 유형
17. 정보보호, 개인정보보호 주관부서는 정보보호 및 개인정보보호 정책, 지침의 변경이 필요한 경우 다음 절차에 따라 변경한다.
18. 실무부서에서 의뢰한 개정 필요성 검토
19. 개정안 작성 및 정보보호 관리자 검토
20. 정보보호위원회 의결 및 최고경영자의 승인
21. 개정된 정책 및 지침 공표 및 교육
22. 정보보호, 개인정보보호 주관부서는 정보보호 및 개인정보보호 정책, 지침의 폐기가 필요한 경우 해당 정책 · 지침의 승인을 받고 폐기할 수 있다. 폐기시 전사 게시 또는 메일로 폐기사실을 관련 부서에 공지하여야 한다.
23. **이행점검**
24. 정보보호, 개인정보보호 주관부서는 정보보호 규정, 유관법률(‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’, ‘개인정보보호법’, '신용정보의 이용 및 보호에 관한 법률', '통신비밀보호법' 등)이 잘 준수되고 있는지 연1회 점검한다.
25. 정보보호, 개인정보보호 주관부서는 이행점검을 위한 기준, 방법, 역할 등 세부 계획을 수립하여 운영한다.
26. 정보보호, 개인정보보호 주관부서는 이행점검 결과를 문서화하여 정보보호 최고책임자, 개인정보 관리책임자에게 보고하고, 발견된 문제점을 조치하여야 한다.
27. 정보보호, 개인정보보호 주관부서는 정부기관의 실태조사, 개인정보 유출사고 등이 발생할 경우에는 별도의 점검을 실시할 수 있다.
28. **정보보호조직 및 개인정보보호조직 관리**
29. **조직체계**
30. 회사의 정보보호 조직은 정보보호 주관부서와 개인정보보호 주관부서로 구성되며, 회사의 모든 업무 영역에 대해 정보보호, 개인정보보호 업무를 유기적으로 관리한다.
31. 회사의 정보보호 조직은 정보보호 활동을 원활히 수행하기 위하여 정보보호 최고책임자, 정보보호 관리자, 정보보호 담당자, 개인정보 관리자, 개인정보 담당자, 물리보안 담당자, 기술보안 담당자로 구성한다. 단, 기술보안 담당자는 그 기능에 따라 서버/PC 담당자, 네트워크 / 보안시스템 담당자, DB / App 담당자로 구분하여 운용할 수 있다.
32. 회사의 정보보호 조직 구성은 다음과 같다.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | |  | | | | **CEO** | | | | | | | | | |  | | | | |  | | | |
|  |  | | | | | | | |  | |  | | | |  | | | | | | | | |  | |
|  |  | | | | | | | |  | |  | | | | **정보보호 위원회** | | | | | | | | |  | |
|  |  | | | | | | | |  | |  | | | |  | |
|  |  | | | | | | | |  | |  | | | |  | | | | | | | | |  | |
|  |  | | | |  | | | |  | |  | | | |  | | | |  | | | | |  | |
|  | **정보보호 최고책임자** | | | | | | | |  | | | | | | **개인정보 관리책임자** | | | | | | | | |  | |
|  |  | | | |  | | | |  | |  | | | |  | | | |  | | | | |  | |
|  | **정보보호 관리자** | | | | | | | |  | | | | | | **개인정보 관리자** | | | | | | | | |  | |
|  |  | | | |  | | | |  | |  | | | |  | | | |  | | | | |  | |
|  | **정보보호 담당자** | | | | | | | |  | | | | | | **개인정보 담당자** | | | | | | | | |  | |
|  |  | | | |  | | | |  | | |  | | |  | | | | |  | | | | |  |
|  | | | | | | | | | | | | |  | | | | | | | | | | | | |
|  | |  | | | | | |  | | | | | | | |  | | | | | | |  | | |
| **서버/PC 담당자** | | | |  | | **네트워크 / 보안시스템 담당자** | | | |  | | | | **DB/App 담당자** | | | |  | | | **물리보안 담당자** | | | | |
|  | | | | | | | | | | | | | | | | | | | | | | | | | |

1. 회사의 정보보호 조직은 정보보호 담당 부서와 정보보호 업무의 기획, 실행, 평가 및 개선 등에 관한 사항을 심의∙조정하기 위한 정보보호위원회가 있다.
2. 보안 사고 발생 시 정보보호 조직을 중심으로 보안사고 대응을 위한 임시 조직이 구성될 수 있다.
3. **정보보호 주관부서**
4. **정보보호 최고책임자**
5. 정보보호 최고책임자는 CEO가 임명하며, 다음 각 호의 자격을 보유하여야 한다.
6. 정보보호 및 개인정보보호와 관련된 법령 혹은 규칙에 대한 높은 이해도
7. 정보자산 및 개인정보자산에 대한 관리적, 기술적, 물리적 보호조치 전략수립 및 이행경험 보유
8. 정보보호 최고책임자는 다음과 같은 업무를 수행해야 한다.
9. 정보보호 활동의 총괄적인 관장
10. 정보보호 규정에 대한 검토 및 승인
11. 정보보호 활동계획 및 이행 여부 확인
12. 정보보호 활동을 정기적으로 CEO에 보고
13. 조직간 보안 Issue 조정 및 보안관리 프로세스 개선
14. 보안관련 대외 접점
15. 전사 보안정책 수립 및 관리 체계 구축 총괄
16. 보안 위기대응 관리체계 구축 및 보안사고 Follow-up 총괄
17. 전사 보안 교육 및 변화 관리 총괄
18. 전사 정기/수시 보안관리 수준 점검 의뢰/협의
19. 정보보호 조직 구성 및 운영 총괄
20. 정보보호 최고책임자는 업무상 필요 시 CEO의 승인을 받아 CIO와 겸직할 수 있다. (잘 못되었다고 할 수도 있고 아니라고도 할 수 있다. 이유 : 45조 3항(정보보호 최고책임자는 업무외의 다른 업무를 겸직할 수 없다라고 내용이 나옴. ) 추가 조항 : 일정 요건에 해당하는 기업만이 겸직할 수 없다. 아니면 겸직할 수 있다.)
21. **정보보호 관리자**
22. 정보보호 관리자는 정보보호 최고책임자가 임명하며 다음 각 호의 자격을 보유하여야 한다.
23. 정보보호 관련 법령에 대한 높은 이해
24. 관리적, 기술적, 물리적 보호조치에 대한 지식 및 경험 보유
25. 정보보호 관리자는 다음과 같은 업무를 수행해야 한다.
26. 정보보호관리체계의 수립 및 관리·운영
27. 정보보호 관리계획 수립 및 시행
28. 정보보호 취약점 분석·평가 및 개선
29. 사전 정보보호대책 마련 및 보안조치 설계·구현
30. 정보보호 사전 보안성 검토
31. 중요 정보의 암호화 및 보안서버 적합성 검토
32. 보안감사 (정보보안 조치점검, 개인정보보호 점검 지시 등)
33. 정보보호 관련 법률 검토 총괄
34. 정보자산에 대한 위험분석 및 관리
35. 주요 정보보호 이슈 파악
36. 개인정보를 포함한 회사의 중요정보 반출에 대한 승인
37. 저장매체에 저장되는 정보에 대한 승인
38. 보안사고에 대한 대응 및 복구 관리
39. **정보보호 담당자**
40. 정보보호 담당자는 정보보호 최고책임자가 임명하고, 정보보호 관련 업무를 지정할 수 있다.
41. 정보보호 관리자는 다음과 같은 업무를 수행해야 한다.
42. 정보보호 관리계획 수행
43. 정보보호 취약점 분석 및 평가
44. 정보보호대책 이행
45. 정보보호 사전 보안성 검토 수행
46. 보안감사 (정보보안 조치점검, 개인정보보호 점검 등)
47. 정보보호 관련 법률 검토
48. 정보자산에 대한 관리
49. 보안사고에 대한 대응 및 복구
50. 교육훈련 관리
51. 보안점검 및 취약성점검
52. **개인정보보호 주관부서**
53. **개인정보 관리책임자**
54. 개인정보 관리책임자는 CEO가 임명하며, 다음 각 호의 자격을 보유하여야 한다.
55. 개인정보보호 관련 법령에 대한 높은 이해
56. 관리적, 기술적, 물리적 보호조치에 대한 지식 및 경험 보유
57. 개인정보 관리책임자는 다음과 같은 업무를 수행해야 한다.
58. 개인정보보호 활동의 총괄적인 지휘 및 감독
59. 개인정보보호 지침서의 유지 및 이행여부 확인
60. 개인정보보호 활동계획 및 이행 여부 확인
61. 개인정보보호 활동을 정기적으로 CEO에 보고
62. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
63. **개인정보 관리자**
64. 개인정보 관리자는 개인정보 관리책임자가 임명하며, 다음 각 호의 자격을 보유하여야 한다.
65. 개인정보보호 관련 법령에 대한 높은 이해
66. 관리적, 기술적, 물리적 보호조치에 대한 지식 및 경험 보유
67. 개인정보 관리자는 다음과 같은 업무를 수행해야 한다.
68. 개인정보 보호 계획의 수립 및 시행
69. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
70. 내부 관리계획 수립 및 시행
71. 개인정보 보호 교육 계획의 수립 및 시행
72. 개인정보파일의 보호 및 관리·감독
73. 개인정보 처리방침의 수립·변경 및 시행
74. 개인정보 보호 관련 자료의 관리
75. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
76. 개인정보 보호조치, 개인정보 점검
77. 고객의 개인정보수집, 이용, 제공 및 관리에 관한 업무를 총괄
78. 회사의 직원 또는 제3자에 의한 위법, 부당한 개인정보의 침해행위에 대하여 관리 감독
79. 고객으로부터 제기되는 개인정보에 관한 대외민원 처리상황의 불만이나 의견의 처리 및 감독을 수행
80. **개인정보 담당자**
81. 개인정보 담당자는 개인정보 관리자가 임명하고, 개인정보보호 관련 업무를 지정할 수 있다.
82. 개인정보 담당자는 다음과 같은 업무를 수행해야 한다.
83. 개인정보 보호 계획의 수행
84. 개인정보 처리 실태 및 관행의 정기적인 조사
85. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
86. 개인정보 보호 교육 계획의 수행
87. 개인정보파일의 보호 및 관리
88. 개인정보 처리방침의 수립·변경
89. 개인정보 보호 관련 자료의 관리
90. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
91. 회사의 소속 직원 또는 제3자에 의한 위법, 부당한 개인정보의 침해행위 관리
92. 고객으로부터 제기되는 개인정보에 관한 대외민원 처리상황의 불만이나 의견의 처리
93. **물리보안 담당자**
94. 물리보안 담당자는 정보보호 관리자가 임명하고, 정보보호 관련 업무를 지정할 수 있다.
95. 물리보안 담당자는 다음과 같은 업무를 수행해야 한다.
96. 출입증 및 출입권한(지문등록 등) 발급 및 이력관리
97. 사무공간 통제 및 관리
98. 자산관리 및 물품의 반출입 통제
99. 주요시설(서버실, 취약성분석실 등)에 대한 출입기록(CCTV녹화, 출입통제장치의 로그기록)에 대한 관리 및 보관
100. 전산장비의 물리적 보호(화재 예방설비(소화기) 구입 및 관리, 출입통제장치 관리 등)
101. **기술보안 담당자**
102. 기술보안 담당자는 정보보호 관리자가 임명하고, 정보보호 관련 업무를 지정할 수 있다.
103. 서버/PC 담당자는 다음과 같은 업무를 수행해야 한다.
104. 서버시스템 계정 관리(계정 발급, 변경 및 삭제)
105. 로그파일에 대한 모니터링
106. 서버/PC의 취약성점검 실시
107. 중요 데이터 및 설정 값에 대한 백업 실시
108. 서버 및 PC 도입을 위한 계획 수립 및 인수
109. 성능 및 용량 관리를 위한 계획 수립 및 모니터링
110. 시각 동기화 및 보안패치 실시
111. 네트워크/보안시스템 담당자는 다음과 같은 업무를 수행해야 한다.
112. 네트워크 및 보안시스템 계정 관리(계정 발급, 변경 및 삭제)
113. 사내 IP주소 기록 및 관리
114. 사내 네트워크 구성 및 변경 관리
115. 로그파일에 대한 모니터링
116. 네트워크 및 보안시스템 취약성점검 실시
117. 중요 장비에 대한 설정 값에 대한 백업 실시
118. 시각 동기화 및 보안패치 실시
119. 무선랜 보안 관리(불법 AP 점검, Ad-Hoc 등)
120. 성능 및 용량 관리를 위한 계획 수립 및 모니터링
121. DB/App 담당자는 다음과 같은 업무를 수행해야 한다.
122. DB 및 어플리케이션에 대한 계정 관리(계정 발급, 변경 및 삭제)
123. 사용자계정관리 및 DB 접근권한관리 등 DBMS 운영업무
124. DB 접근권한 부여에 대한 적정성 검사
125. 로그파일에 대한 모니터링
126. 중요 DB 및 어플리케이션에 대한 백업 실시
127. DB 및 어플리케이션에 대한 취약성점검 실시
128. 개인정보 및 중요정보에 대한 암호화 및 암호키 관리
129. 성능 및 용량 관리를 위한 계획 수립 및 모니터링
130. **구성**

정보보호 및 개인정보보호 업무의 기획, 실행, 평가 및 개선에 관한 사항을 심의 조정하기 위해 정보보호위원회를 다음 각 호와 같이 구성한다.

1. 위원장: 정보보호 최고책임자
2. 위원: 구매 관리 본부 본부장, 마케팅 본부 본부장, 고객 관리 본부 본부장, 인프라 본부 본부장, 물류 관리 본부 본부장
3. 간사: 정보보호 관리자
4. 기타 정보보호위원회의 사안에 따라 관련 부서장 및 담당자가 정보보호 위원회에 참석할 수 있다.
5. **임무**

정보보호위원회는 다음 각 호의 사항에 대해 심의 조정한다.

1. 정보보호 및 개인정보보호 정책 및 지침의 제정, 개정 및 폐지에 관한 사항
2. 정보보호 및 개인정보보호 계획 검토 및 자원 배분에 관한 사항
3. 보안사고 처리 검토 및 재발 방지 대책 협의
4. 정보보호 및 개인정보보호 대책 및 시스템의 개선과 발전에 관한 사항
5. 정보보호실무반으로부터 부의된 사항
6. 정보보호 및 개인정보보호 실천 우수자 또는 위반자에 대한 상벌 사항 결정
7. 기타 위원장이 필요하다고 판단된 안건
8. **운영**

정보보호위원회(개인정보보호위원회 포함)는 다음 각 호와 같이 운영한다.

1. 위원장은 회의를 연 1회 소집한다. 다만, 중대한 사항 발생 시 임시 소집할 수 있다.
2. 정보보호위원회를 소집할 경우 간사는 안건, 장소, 일정, 참석대상을 사전 공지한다.
3. 위원회의 의결은 긴급을 요하거나 기타 위원장이 필요하다고 인정한 경우에는 서면이나 전자결재에 의한 결의로써 갈음할 수 있다.
4. 위원장이 부득이한 사유로 인하여 직무를 수행할 수 없는 경우 위원장이 미리 지명한 위원이 그 직무를 수행할 수 있다.
5. 정보보호위원회의 효율적인 운영을 위하여 정보보호실무반을 운영한다.
6. 정보보호위원회는 구성위원의 과반수 이상 출석으로 개최하고, 출석위원 과반수 찬성으로 의결하며, 위원회가 가부동수인 경우 위원장이 결정권을 갖는다.
7. 정보보호위원회의 결정사항에 중대한 착오가 발견되거나 재심 요구가 있을 때에는 위원장은 지체 없이 회의 소집 등 재심의에 필요한 조치를 해야 한다.
8. 간사는 위원회의 결정사항이 승인을 받아 확정되면 이를 관련 부서에 지체 없이 통보해야 한다.
9. 정보보호위원회에 관여한 자는 정보보호위원회에서 심의된 사항 중 비밀에 속하는 사항을 누설하거나 공개되지 않도록 비밀을 유지해야 한다.
10. **보안사고 대응반**
11. **구성**
12. 보안사고를 인지한 회사의 임직원은 관련 사실을 정보보호 담당부서에 신고한다.
13. 정보보호 담당부서는 보안사고 파악한 후 보고체계에 따라 경영층에 보고하며 관련 부서에 전파를 하여야 한다.
14. 보안사고 대응반에 참여하는 관련 부서는 다음 각 호와 같으며 각 부서별 역할에 따라 긴급대응을 실시한다.
15. 정보보호 담당부서
16. 개인정보 담당부서
17. 대외협력 관련부서
18. 고객 서비스부서
19. 서비스 개발부서
20. 서비스 운영부서
21. 경영지원 및 인사 관련 부서
22. 정보보호 담당자 및 개인정보 담당자는 보안사고 발생 시 신속한 대응을 위해 비상연락 체계를 마련해야 하며, 최신의 상태를 유지하여야 한다
23. **임무**

보안사고 대응반은 보안사고 발생 시 다음 각 호의 업무를 수행한다

1. 보안사고 발견 시 초기 대응
2. 보안사고 대응을 위한 기술 지원 및 분석, 취약점 제거 방안 제시
3. 보안사고의 사후처리
4. 고객/대외기관 및 언론 대응, 법적 처리 등의 업무
5. **운영**
6. 보안사고 대응반은 보안사고 발생 시 정보보호 관리자에 의해 소집된다.
7. 보안사고 대응반은 보안사고 대응 결과의 보고 및 복구 완료 시점까지 한시적으로 운영된다.
8. **정보자산 위험관리**
9. **정보자산 및 개인정보자산관리**
10. **자산의 식별 및 분류**
11. 정보자산은 다음과 같은 유형으로 분리하여 식별하여야 한다.
12. 정보처리시스템이란 서비스 제공을 위한 서버, 네트워크 장비, 응용프로그램 등을 말하며, 응용시스템, IT Infra(서버, 네트워크/보안장비), 기타(PC, OA시스템)으로 구분한다.
13. 문서란 영업 정보, 고객 정보, 계약서, 매뉴얼 등의 전자적 형태 및 종이 형태로 저장되는 정보자산을 말한다.
14. 정보보호 관리자는 연 1회 부서 별 정보자산목록을 기준으로 회사의 정보자산 목록을 작성 및 유지하여야 한다.
15. **정보자산목록 작성 및 유지**
16. 정보보호 관리자는 정보자산 목록을 작성 및 유지하고 매년 말 갱신하여야 한다.
17. 정보자산 목록에 사용되는 정보자산 분류 코드는 “정보자산 코드표”에 따라 부여한다.
18. 정보보호 관리자는 각 부서장에게 정보자산 목록 작성을 요청할 수 있고, 요청 시 각 부서장은 반드시 응해야 한다.
19. **정보자산 가치평가**
20. 정보자산은 중요도와 속성 가중치에 따라 그 가치를 평가하여 다음의 각 호에 따른다.
21. 중요도
22. 3.0: 정보자산이 포함하고 있는 정보항목 중 등급이 High인 정보항목이 1개 이상을 포함하고 있는 경우
23. 2.0: 정보자산이 포함하고 있는 정보항목 중 등급이 High인 정보항목은 없으며, Medium인 정보항목이 1개 이상을 포함하고 있는 경우
24. 1.0: 정보자산이 포함하고 있는 정보항목이 Low 등급만 포함되어 있는 경우
25. 속성 가중치
26. 2.0: 기밀성, 무결성, 가용성의 정보 속성이 모두 보장되어야 하는 정보자산 (C, I, A가 모두 해당되는 자산)
27. 1.5: 기밀성, 무결성, 가용성 중 2개의 정보 속성이 보장되어야 하는 정보자산 (C, I, A 둥 2개만 해당되는 자산)
28. 1.0: 기밀성, 무결성, 가용성 중 1개의 정보 속성이 보장되어야 하는 정보자산 (C, I, A 중 하나만 해당되는 자산)
29. 가치평가는 다음의 공식에 따른다.

***정보자산 가치 : 정보 중요도 X 속성 가중치***

1. 정보보호 관리자는 정보자산 가치평가의 기준이 되는 정보항목의 유형을 “정보항목 유형”의 양식에 따라 작성 및 유지하여야 한다.
2. 각 부서의 장은 정보보호 관리자에게 정보항목의 유형을 조정 요청할 수 있으며, 정보보호 관리자는 각 부서장의 정보항목 유형 조정 요청에 대하여 검토 후 조정하여야 한다.
3. **정보시스템 목록 작성 및 유지**
4. 정보보호 관리자는 정보시스템의 목록을 유지하여야 한다.
5. 정보보호 관리자는 각 기술보안 담당자에게 정보시스템 목록 작성을 지시할 수 있으며, 각 기술보안 담당자는 정보보호 관리자의 정보시스템 목록 작성 지시에 응해야 한다.
6. **문서 분류**

문서는 '비밀', '대외비', '일반' 문서로 보안등급을 분류하며, 분류 기준은 다음과 같다.

1. 비밀(Secret): 회사의 영업활동이나 내부 관리와 직접적인 관련이 있으며, 유출될 경우 영업을 중지하거나 벌금이상의 처벌이 가해져 심각한 피해가 예상되는 정보자산, 정보자산 가치평가 기준에 따라 ‘High’ 정보항목이 1개 이상인 정보
2. 대외비(Confidential): 회사의 영업과 간접적인 관련이 있으며, 유출될 경우 대외 신임의 하락이나 차기 프로젝트에 약간의 지장이 발생 가능한 다소 피해가 예상되는 정보자산. 단, 외부 발표용 자료는 대외비로 한다. 정보자산 가치평가 기준에 따라 정보항목이 ‘High’는 없으며 ‘Medium’이 1개 이상인 정보
3. 일반: 회사의 영업과 관련이 있으며, 유출되어도 회사에 미치는 영향이 미미한 정보자산, 정보자산 가치평가 기준에 따라 정보항목이 ‘Low’만 존재하는 정보
4. **문서 관리**
5. 모든 정보자산은 생산하거나 수집한 부서에서 담당자를 지정하여 저장 및 보관하여야 한다.
6. 정보자산 소유 부서장은 파일서버 및 외부 저장장치를 이용하여 정보자산을 저장 및 보관하고, 비밀 등급이며 data 형태인 정보자산은 암호화 후 저장 및 보관해야 한다.
7. 일반 임직원의 문서와 개발자의 소스코드 암호화는 회사 지정방법을 따르도록 한다.
8. 정보자산을 저장 및 보관하는 경우 이용 권한이 없는 인력이 해당 정보자산에 접근할 수 없도록 접근 및 권한관리 대책을 강구하여 적용하여야 한다.
9. 정보자산이 인쇄문서, USB 등 외부저장매체와 같이 유형화된 형태로 보관하는 경우에는 잠금장치가 있는 장소 혹은 캐비닛 등에 보관하여야 한다.
10. 생성 중이거나 결재중인 정보자산은 결정된 보안등급에 따라 완료된 상태의 보안등급에 준하여 관리되어야 한다. 단, 반려 등으로 활용하지 않을 정보자산은 즉시 폐기하여야 한다.
11. **저장매체 관리**
12. 회사내부 정보처리시스템의 저장장치를 폐기하거나 재사용할 경우에는 데이터의 완전 삭제에 대한 확인을 받아야 한다.
13. 외부 업체를 이용하여 저장장치를 폐기하거나 재사용할 경우에는 데이터의 완전 삭제에 대한 확인을 받아야 한다.
14. **위협의 식별 및 평가**
15. **위협의 식별**
16. 정보보호 관리자는 회사의 리서치 조직을 활용하여 위협을 식별하고 식별된 위협에 대한 평가를 수행하여야 한다.
17. 위협은 관리적, 물리적, 기술적으로 현재 발생한 모든 위협을 조사하여 발생 빈도를 도출하여야 한다.
18. 정보보호 관리자는 “위협의 유형”의 양식에 따라 위협 목록을 유지한다.
19. **위협의 빈도 평가**

위협의 빈도는 다음 각 호의 기준에 따라 평가한다.

1. High : 발생 가능성 높음 (80% 이상의 확률로 발생이 예상됨)
2. Medium : 발생 가능성 존재함 (60% 이상의 확률로 발생이 예상됨)
3. Low : 발생 가능성 낮음 (60% 미만의 확률로 발생이 예상됨)
4. **취약성 진단 및 평가**
5. **취약성 진단**
6. 정보자산에 대한 취약성은 관리적 취약성과 기술적 취약성으로 구분하여 진단한다.
7. 정보보호 관리자는 매년 관리적 취약성을 진단하여야 하며, 기술보안 담당자(서버/PC, 네트워크/보안시스템, DB/App 담당자)에게 지시하여 기술적 취약성을 진단하도록 지시한다.
8. 관리적 취약성 진단은 정보보호 관리자가 지정한 정보보호 관리체계 인증기준 중 하나를 지정하여 사용하며 특별한 지정이 없으면 KISA-ISMS를 기준으로 한다.
9. 기술적 취약성 진단의 기준은 기술보안 담당자가 기준표를 작성하고 연 1회 정보보호 관리자에게 보고하여야 한다.
10. **취약성 진단 결과의 유지 및 활용**
11. 정보보호 관리자는 취약성 진단 결과를 유지하여야 한다.
12. 취약성 진단 결과는 정보자산에 대한 위험분석에 활용한다.
13. 취약성 진단 결과는 임의로 외부에 공개할 수 없다. 단, 정보보호 최고책임자의 승인이 있는 경우는 예외로 한다.
14. **위험분석**
15. **위험도 측정**
16. 정보보호 관리자는 정보자산의 가치, 위협의 빈도, 취약성의 정도를 활용하여 위험도를 측정하여야 한다.
17. 정보보호 관리자는 각 부서의 위험분석을 각 본부장에게 의뢰할 수 있으며, 의뢰 받은 각 본부장은 해당 본부의 위험분석을 수행하여야 한다.
18. 정보보호 관리자는 연 1회 위험분석을 수행하고 그 결과를 정보보호 최고책임자에게 보고하여야 한다.
19. **허용가능 위험도의 결정**
20. 위험도 산출이 완료된 경우 정보보호 관리자는 허용 가능한 위험 정도 (DoA, Degree of Assurance)를 결정하여 정보보호 최고책임자에게 보고해야 한다.
21. 정보보호 최고책임자는 DoA 의견을 받아 정보보호 위원회의 상정하여 결정하고 승인한다.
22. **보호대책 수립 및 이행**
23. **보호대책의 수립 및 공표**
24. 정보보호 최고책임자는 각 본부장과 함께 위험도 산출 및 DoA 결정에 따라 관리하여야 할 위험에 대한 보호대책을 수립하여야 한다.
25. 수립된 보호대책은 그 효율, 소요비용, 적용 용이성 등의 항목으로 우선순위를 정해야 한다.
26. 정보보호 최고책임자는 우선순위가 정의된 보호대책은 각 본부장 및 자산의 소유자에게 공표하여야 한다.
27. 보호대책은 기능, 성능, 호환성 등 기술적 요인 이외에 재정적, 법/제도적, 문화적 제약조건들을 고려하여 수립하여야 한다.
28. 관리계획에는 우선순위, 일정, 예산, 책임, 운영계획 등이 포함되도록 수립한다.
29. 보호대책은 적절한 관리조치와 우선순위에 따라 일관성 있게 수립되어야 하며 수립의 정확성에 대한 검토 결과를 문서화 하고 유관담당자에게 내용을 공유하여야 한다.
30. **보호대책의 이행**
31. 정보보호 최고책임자는 보호대책이 원활히 이행될 수 있도록 관리계획을 수립하고, 수립된 관리계획에 따라 누락 없이 이행하여야 한다.
32. 정보보호 최고책임자는 관리계획이 누락 없이 이행되고 있는지에 대하여 반기 1회 이행수준을 점검하고 미 이행되거나 이행이 더딘 관리계획에 대한 수정계획을 수립하여 적용하여야 한다.
33. **사후관리**
34. **관리체계의 재검토**
35. 정보보호관련 대내외 환경변화가 조직에 미치는 영향을 분석하며, 또한 내부감사 지적 사항과 보안사고의 영향을 반영할 수 있도록 재검토 하여야 한다.
36. 재검토는 다음과 같은 내용을 포함하여야 한다.
37. 정책의 효율성
38. 정책의 적절성
39. 잔류위험의 수준
40. 절차 등
41. **관리체계의 모니터링 및 개선**
42. 관리체계는 회사의 목적과의 일치성을 만족시키기 위하여 정보보호 관리자에 의해 지속적으로 모니터링 되어야 한다.
43. 정보보호 관리자는 관리체계의 정보보호 활동 모니터링 결과를 정보보호 최고책임자에게 보고하여야 한다.
44. 정보보호 최고책임자는 모니터링 결과를 분석하여 개선사항을 도출하고, 이행할 수 있는 절차를 수립하여야 한다.
45. **위험관리전략 및 계획수립**
46. 전략 및 계획은 회사의 목표 및 정책, 법적 요구사항을 고려한다.
47. 위험관리 계획은 적절한 기간과 예산을 고려하여 수립한다.
48. 회사는 적합한 위험관리를 수행하기 위하여 위험관리 전략 및 계획에 조직, 역할과 책임, 주요 위험관리 과정 등을 포함하여야 한다.
49. 위험관리 조직은 한시적으로 전담반이 구성되는 것을 원칙으로 하며 해당 부서의 실무 책임자가 참여해야 한다.
50. 위험분석 범위는 회사의 사업분야/방향, 산업특성, 법적 규제 등을 고려하여 선정한다.
51. 위험분석 방법은 내ㆍ외적인 환경변화에 대응할 수 있도록 매년 검토한다.
52. **생활환경보안**
53. **업무환경보안**
54. **개인정보 환경보안**
55. 정보보호 주관부서는 회사에서 지급한 PC(이하 '업무용 PC'라 한다)에 백신 프로그램, 문서보안 프로그램 등 보안프로그램이 설치되도록 하여야 하며, 미설치된 업무용 PC에 대해 네트워크 이용을 제한할 수 있다. 단, 업무상 필요할 경우에는 예외처리한다.
56. 정보보호 주관부서는 업무용 PC의 보안설정 여부, 클린데스크 등을 정기적으로 점검하고, 그 결과를 정보보호 최고책임자에게 보고하여야 한다.
57. 정보보호 주관부서는 모든 업무용PC에 백신프로그램, 보안 패치가 설치되도록 하여야 하며, 백신프로그램은 자동 업데이트 및 실시간 감시 기능이 활성화되도록 하여야 한다.
58. 정보보호 주관부서는 임직원으로부터 바이러스, 악성코드 등의 감염 신고를 받을 경우에는 즉시 조치를 취하여야 한다.
59. 정보보호 주관부서는 다음과 같은 비업무용 인터넷 사이트의 접근을 차단하여야 하며, 이에 대해 모니터링할 수 있다.
60. 불건전 음란 정보, 증권정보, 게임을 포함하는 사이트
61. 악성코드 유포, 스팸메일 발송 등 불법행위를 시도하는 사이트
62. 웹하드, P2P 등 사용시 회사의 정보 유출이 우려되는 사이트
63. 기타 정보보호 주관부서에서 보안상 차단이 필요하다고 판단하는 사이트
64. 정보보호 주관부서는 불법 소프트웨어의 사용을 주기적으로 점검하고 조치하여야 한다.
65. **공용업무 환경보안**
66. 물리보안 담당자는 복사기, 프린터 등의 공용사무기기에 대하여 관리하여야 한다.
67. 공용 PC는 업무용 PC와 동일한 수준의 보안설정을 적용하여야 한다.
68. **물리적 보안**
69. **보호구역의 지정**
70. 정보보호 최고책임자는 회사의 주요 정보자산 및 관련 시설에 대한 보안강화를 위하여 다음 각 호와 같은 보호구역을 지정 및 운영하여야 한다.
71. 제한구역: 회사의 중요정보가 사용되어 임직원은 출입 가능하나, 외래인 및 방문자에 대한 출입 안내가 요구되는 구역
72. 통제구역: 회사의 핵심적인 정보가 사용 및 보관되어 임직원 또한 출입 허가를 득한 자만 출입이 가능한 구역
73. 지정된 보안구역은 “보안구역 현황”에 따른다.
74. **제한구역의 통제**
75. 정보보호 최고책임자는 제한구역의 출입통제를 위하여 카드 잠금장치, 지문인식 잠금장치 등 출입통제 장치를 설치 및 운영하여야 한다.
76. 제한구역을 출입하는 모든 출입자는 반드시 출입증을 패용하여야 한다.
77. 외부인력의 제한구역 출입은 업무상 필요에 따라 결정되어야 하며, 수행직원은 외부인력과 동행하여 제한구역에서의 활동을 지속적으로 감독하여야 한다.
78. **휴대용 전산장비의 반/출입**
79. 회사에서 근무하는 모든 인력은 회사 전산장비에 임의로 휴대용 전산장비 또는 저장매체를 부착 또는 제거할 수 없다.
80. 휴대용 전산장비를 외부에서 사용하기 위해서는 다음 각 호를 준수하여야 한다.
81. 모든 휴대용 전산장비는 공공장소(호텔, 자동차, 비행기, 회의장 등)에 홀로 남겨두어서는 안 되며 도난으로부터 보호할 수 있도록 가방, 금고, 잠금장치 등에 의해 보호해야 한다.
82. 휴대용 전산장비는 여행 중 항상 위치 확인이 가능한 곳에 보관하여야 한다.
83. 모든 사용자는 휴대용 전산장비를 사용할 때 작업 내용이 타인에게 노출되거나 보이지 않도록 주의하여야 한다.
84. 휴대용 전산장비를 외부에서 사용 중 분실하였을 경우 즉시 소속 팀장 및 정보보호 관리자에게 통보하고 찾을 수 있도록 조치를 취하여야 한다.
85. 정보보호 관리자는 분실된 휴대용 전산장비에 포함된 정보자산을 보호할 수 있도록 대책을 수립하여야 한다.
86. **영상정보 보안**
87. 물리보안담당자는 영상기기를 통하여 회사 내 중요시설의 이상 유무를 확인함으로써 미연에 사고를 방지하여야 한다. 영상기기를 설치할 경우 영상기기 촬영 안내판을 설치하여야 한다.
88. 물리보안담당자는 영상기기가 항상 정상 가동상태로 유지되도록 점검하여야 하며 기기 장애 발생 시에는 즉시 수리 의뢰 조치하여야 한다.
89. 주요시설의 출입구와 주요시설 중 전산실 및 취약점분석실 내부에 영상기기를 설치해야 한다.
90. 영상기기의 녹화 자료는 250GB의 용량을 초과하면 자동 삭제하여야 한다.
91. **케이블 보안**
92. 배전반, 전화 단자함 등은 잠금장치를 설치하는 등 인가된 자에 한해 접근이 가능하도록 관리하여야 한다.
93. 전산장비에 연결된 전력과 통신 케이블은 절단 등의 위협으로부터 보호하기 위해 가능한 매설하고, 매설이 어려울 경우 보호용 파이프 등을 사용하여 보호해야 한다.
94. 일반구역이나 케이블이 외부에 노출 될 위험이 예상되는 지역은 우회하여 케이블을 설치한다.
95. **전원관리**
96. 일시적인 전력 중단이나 기타 전기적 이상으로부터 가용성을 확보하기 위해 대체 전력 공급원을 확보하여야 한다.
97. **인력보안**
98. **주요직무자의 지정**

주요 직무자의 기준은 다량의 개인정보 처리자와 시스템 관리자 등 주요 직무자를 정의 및 지정하고, 현황을 관리하여야 한다.

1. **입퇴사 관리**
2. 인사 주관부서는 임직원의 입사 시 회사 내 정보보호 책임이 명시된 정보보호 서약서, 개인정보보호 서약서를 징구하여야 한다.
3. 인사 담당자는 임직원의 부서 이동 시 해당 사항을 공지하여야 한다.
4. 회사의 부서장은 임직원의 부서 이동에 따른 업무 변경 시 IT 인프라 및 서비스에 존재하는 계정 및 권한 삭제 등을 수행하여야 한다.
5. 임직원의 부서 이동 시 기존에 사용하던 IT인프라, 서비스의 계정 및 권한이 업무상 필요한 경우 이동될 부서에서 신청하여 부여 받아야 한다
6. 인사 담당자는 임직원 퇴사 시 퇴직자 서약서, 비밀유지 서약서를 징구하고, 회사 재산 회수∙반납 확인서 등 관련 서류를 확인한 후 퇴사처리를 수행한다.
7. 인사 담당자는 퇴사자 발생 시 퇴사자 명단을 다음 부서에 통보하여야 한다.
8. 사옥 시설관리 부서
9. IT 인프라 운영 부서
10. 정보보호 전담 부서
11. 정보보호 담당자는 정기 보안 감사를 통해 퇴사자에 대한 보안통제가 적용되었는지 확인하여야 한다.
12. **교육훈련**
13. **정보보호 교육계획의 수립**
14. 정보보호 담당자 다음 각 호를 고려하여 회사 임직원의 정보보호 교육을 계획한다.
15. 교육 대상 및 목적
16. 교육 내용: 법에서 정하는 내용 (예: 개인정보의 안전성 확보조치기준 등)
17. 교육 일정 및 시간
18. 교육 방법
19. 교육 내용 및 강사 평가 결과
20. **교육대상**
21. 정보보호 담당자는 모든 임직원과 3개월 이상 회사에 상주하여 업무를 수행하는 외부인에 대한 연 1회 정보보호 교육을 실시하여야 한다.
22. 신규 입사자는 입사 후 3개월 이내에 정보보호 교육을 수료하여야 하며, 외부인의 경우 회사의 출입증을 발급받은 1개월 이내에 정보보호 교육을 수료하여야 한다.
23. 정보보호 담당자는 정보보호 교육 실시 후 교육 결과를 관련 부서에 전달한다.
24. **교육의 시행**
25. 정보보호 담당자는 사용자의 부주의나 고의에 의한 정보보호 사고를 최소화하기 위해 다음 각 호와 같이 정기 교육 및 비정기 교육을 실시한다.
26. 정기 교육은 연 1회 실시
27. 비정기 교육은 정보보호사고 발생 후 사고에 대한 내용과 대응절차에 대한 교육이 필요한 경우, 새로운 정보보호 이슈에 대한 교육이 필요하다고 인정되는 경우, 실무 부서에서 교육의 필요성이 제기되는 경우일 때 실시
28. 정보보호 담당자는 사내 게시판이나 메일 등을 활용하여 임직원의 정보보호 인식제고를 위한 홍보를 지속적으로 실시하여야 한다.
29. **개발 및 IT 인프라 운영보안 관리**
30. **개발 및 운영 관리**
31. **직무분리**

정보처리시스템의 운영과 개발, 정보보호시스템 운영 등 업무별 직무를 분리하여 권한의 오남용을 방지하여야 한다, 단, 직무분리가 불가능할 경우에는 직무자의 책임추적성 확보를 위한 보완통제를 적용하여야 한다

1. **개발 관리**
2. 개발조직은 어플리케이션 개발 · 변경 기획단계에서 다음 각 호의 보안 요구사항을 상세 파악하여 프로그램에 반영하여야 하며, 개발완료 시 개발검증자를 통해 보안요구사항을 만족하였는지 확인하여야 한다.
3. 사용자 식별 및 인증
4. 권한관리 및 접근통제
5. 암호화 등 주요정보의 기밀성과 무결성을 확보할 수 있는 방안
6. 로깅기록 및 감사
7. 장애 발생 시 가용성 확보
8. 클라이언트 통제
9. 개발조직은 어플리케이션 설계 · 개발 시 중대한 보안위험이 판단되는 경우 정보보호 최고책임자에게 보안성 심의를 요청하여야 한다.
10. 개발조직은 시스템계정, DB 테이블, 개발 프로그램 등의 권한을 받기 위해서 정보보호 최고책임자의 승인을 받아야 한다.
11. 정보보호 관리자는 개발자 별로 접근권한을 설정하고 그 사실을 기록 · 관리해야 한다.
12. 개발조직은 운영시스템에서 어플리케이션을 개발 또는 변경할 수 없다.
13. 운영시스템에는 개발 중인 소스코드나 목적코드를 저장할 수 없다.
14. 개발조직은 개발 중인 프로그램에 대한 버전을 관리하여야 하며, 운영시스템 프로그램 변경버전에 대해 보관 · 관리하여야 한다.
15. 개발조직은 어플리케이션 개발 테스트 시 개인정보 데이터는 개인을 식별할 수 없도록 변환 후 사용하여야 한다. 단, 외부기관과의 테스트 등으로 인해 실 데이터를 통해 테스트를 하여야 하는 경우 개인정보 관리책임자의 승인을 받아 사용하고, 사용완료 즉시 실 데이터를 삭제하여야 한다.
16. 정보보호 최고책임자는 IT개발기획분석 / 개발검증 / QA를 담당하는 임직원(이하 “검수인력”이라 한다)을 지정하여 검수인력으로 하여금 QA업무를 수행하도록 해야 한다.
17. 검수인력은 어플리케이션에 보안대책이 필요하다고 판단되는 경우 정보보호 최고책임자 및 개발조직에 해당사항을 요청할 수 있다.
18. 응용시스템의 운영 시작 전에 필요한 시험과 사용자의 인수 확인이 이루어져야 한다.
19. 개인정보처리시스템 개발 및 개선 계획 시 개인정보 영향평가를 수행하여야 한다.
20. **IT 인프라 보안 관리**
21. 운영지침 및 절차는 문서화되어 있으며 정보보호 최고책임자로부터 승인을 획득하여야 한다.
22. 운영지침서 및 절차서는 다음과 같은 내용을 포함하고 있어야 한다.
23. 정보처리 및 취급 요구사항
24. 오류 및 예외사항 처리지침
25. 예기치 않은 운영적, 기술적 문제 발생시 비상연락망
26. 시스템 문제 발생시 시스템 재 동작 및 복구절차
27. 시스템 모니터링 방안 등
28. 운영관리를 외부에 용역을 주는 경우 계약서에 운영지침에 관련된 항목들과 이를 감사할 수 있는 항목들이 반영되어야 한다.
29. 외부계약자가 정보시스템 및 장비를 관리하는 경우 보안위협과 대책을 계약서상에 반영하여야 한다.
30. **정보처리시스템 및 개인정보처리시스템 관리**
31. **접근통제**
32. 정보 및 응용프로그램 기능의 접근은 응용프로그램 접근통제 정책에 따라 제한하여야 한다.
33. 중요시스템은 전용 컴퓨터 환경에서 수행함으로써 다른 프로세스가 가용성이나 비밀성, 무결성에 영향을 미치는 일이 없도록 하여야 한다.
34. 개인정보를 처리하는 응용프로그램에서 불필요한 기능을 제공하여 권한을 우회할 수 없도록 조치하여야 하고, 우회방법이 존재할 경우 이를 방지하는 대책을 수립하여야 한다.
35. 중요 정보의 출력물에는 표지에 등급과 지정 배포처, 경고문 등이 표시되어야 하며 각 장마다 등급 및 문서번호를 표시하여야 한다.
36. 일정시간 동안 입력이 없는 세션은 Time-out 설정을 통해 연결을 차단하여야 한다.
37. 중요한 응용 프로그램은 동일 사용자의 동시 세션 수를 제한하여 비인가된 접근을 검출할 수 있어야 한다.
38. **이동 컴퓨터 및 원격작업**
39. 이동컴퓨터 보안 정책에 다음과 같은 내용을 포함한다.
40. 이동컴퓨터의 사용
41. 물리적보호, 접근제어, 암호화, 백업, 바이러스 정책
42. 내부네트워크와의 연결
43. 이동컴퓨터 사용자에 대한 보안교육을 실시하여야 한다.
44. 원격작업 시 보안정책과 절차를 수립하여야 한다.
45. 재택근무시 관련 물리적 보안 환경에 대한 지침이 정의되어 있고, 재택근무자가 이 지침을 숙지하며 이에 따른 근무환경을 구성하여야 한다.
46. 이동컴퓨터의 분실시 정보의 유출 방지를 위한 암호화, 장비보호를 위한 물리적 로깅장치, 분실 컴퓨터의 추적 등의 대책을 수립해야 하고, 주요 이동컴퓨터에 대해서는 강화된 보안대책을 수립하여야 한다.
47. 원격작업의 기간이 완료되었을 경우 접근권한, 장비 등을 회수하여야 한다.
48. **보안성 심의**
49. 보안성 심의 대상은 다음과 같다.
50. 업무시스템 및 개인정보 처리시스템에 대한 보안성 확보가 요구되는 경우 정보보호 관리자에 요청하여 보안성 심의를 받아야 한다. 단, 개인정보 처리시스템의 경우 개인정보 영향평가로 대체할 수 있다.
51. 다음과 같이 중요한 사안에 대해서는 정보보호 최고책임자의 보안성 심의를 받아야 한다.
52. 내부 시스템이 외부 기관의 시스템과 데이터 전송을 위하여 최초로 연동되는 경우
53. 내부 시스템이 외부 기관의 시스템과 연동 후 추가로 개인정보를 송수신하는 경우
54. 외부 네트워크 및 DMZ를 통해 외부로 공개되는 시스템(공개용 웹서버 포함) 및 네트워크 장비를 설치하는 경우
55. 협력업체, 외부 유지보수 업체 등이 외부 네트워크로부터 원격접속을 통해서 서비스를 제공하는 경우
56. 개인정보 등 중요한 정보를 저장 · 관리하는 시스템을 도입하는 경우
57. 보안장비 및 암호 프로그램 등 정보보호 시스템을 도입하는 경우
58. 시스템 OS 또는 소프트웨어 등에서 제공하거나, 응용 프로그램 개발을 통해 제작된 보안 유틸리티를 설치 · 실행하고자 하는 경우
59. IT개발 및 운영업무의 일부 또는 전체를 외부에 용역 · 의뢰하는 경우
60. IT운영 · 개발 업무 수행 시 보안에 중대한 영향이 있을 것으로 판단되는 경우
61. 기타 정보보호 최고책임자가 심의한 사항에 대하여 변경이 필요한 경우
62. 기타 경미한 사안에 대해서는 담당 부서장의 결정으로 보안성 심의를 대체할 수 있다. 단, 담당 부서장의 결정으로 보안성 심의를 대체하는 경우 정보보호 최고책임자의 승인을 받아야 한다.
63. 보안성 심의 절차는 다음과 같다.
64. IT보안성 심의 절차는 “보안성 심의 프로세스”를 따른다.
65. 정보보호 최고책임자는 특별한 사유가 없는 한 보안성 심의 요청일 즉시 심의를 진행하여야 한다.
66. 정보보호 최고책임자는 심의 결과에 추가적인 보안대책을 마련하도록 요청할 수 있다.
67. 정보보호 최고책임자는 검토자료가 불충분한 경우 추가자료를 요청할 수 있다.
68. **접속기록의 관리**
69. 정보보호 관리자는 시스템, 네트워크, DB, 어플리케이션에서 발생하는 로그에 대해 기록 · 관리를 주관하여야 한다.
70. 기술보안 담당자는 정해진 기준에 따라 로그가 생성되도록 시스템을 설정하고, 로그 파일에 일반 사용자 또는 비인가자가 접근하지 못하도록 설정하여야 한다.
71. **제3자 서비스 수행관리**
72. 제3자(외부계약자)와 전산운영 및 개발과 관련한 서비스 수행 계약 시, 서비스의 정의 및 역할, 정보보안 준수사항, 책임 및 손해배상에 대한 내용이 계약서 내에 포함되어야 하며 관리, 감독권에 대한 내용도 명시되어야 한다.
73. 제3자에 의하여 제공되는 서비스는 주기적인 감시, 감독이 되어야 하며, 기록 · 관리되어야 한다.
74. 제3자 서비스의 변경 관리(조직은 위험의 재평가와 관련된 사업 시스템 및 프로세스의 중요도를 고려하여 기존의 정보보호 정책의 유지/개선을 포함한 서비스 공급에 대한 변경을 관리하여야 한다.)
75. **성능 및 용량관리**
76. 정보보호 관리자는 부족한 성능 및 용량으로 인한 실패를 회피하기 위해서 계획을 수립하여야 한다.
77. 현재 장비의 성능 및 용량이 요구되는 사용자의 수준을 만족시켜야 한다.
78. 기술보안 담당자는 성능 및 용량의 현황과 요구사항을 분기 1회 모니터링하고 기록 및 분석하여 향후 계획 수립에 반영이 되도록 정보보호 관리자를 지원하여야 하며 개선이 필요할 경우 이에 따라 조정하여야 한다.
79. **장애관리**
80. 업무주관 부서는 정보시스템에 장애 발생 시 즉시 해당 기술보안 담당자에 이를 접수하여야 한다.
81. 해당 기술보안 담당자는 장애발생을 인지하는 즉시 효과적인 장애대응을 위해 업무주관 부서와 함께 비상대응체계를 구축한다.
82. 비상대응체계에 속한 모든 단위조직은 신속한 장애대응을 위해 적극적으로 협조하여야 한다.
83. 기술보안 담당자는 장애조치 후 장애영향도 및 조치내역에 대해 업무주관 부서에 통지해야 한다.
84. 기술보안 담당자는 장애조치 후 장애원인, 조치내역, 향후 개선방안 등 장애예방 및 사후관리에 필요한 정보를 포함한 장애보고서를 작성하여야 한다.
85. **암호화**
86. **암호화 대상**
87. 업무위탁회사, 제휴사, 고객사 등 외부기관과 파일형태로 정보를 제공하는 개인정보는 암호화하여야 한다.
88. “제25조 문서분류”에서 지정한 보안등급에 따라 비밀 이상의 보안등급을 갖는 정보자산은 암호화하여 저장 · 관리하여야 한다.
89. 암호화 대상 정보는 전용선, 인터넷 등 통신망의 보안 취약성에 상관없이 암호화하여야 한다.
90. 제1항 ~ 제3항에도 불구하고 정보보호 최고책임자의 승인을 받은 경우에는 암호화 대상에서 예외로 인정할 수 있다.
91. 정보보호 최고책임자는 회사 내부 또는 외부에서 암호화가 필요하다고 판단되는 정보, 통신구간, DB 테이블 등에 대해 암호화 관리를 요구할 수 있다.
92. 각 부서장은 해당 부서에서 관리하고 있는 주요 정보에 대하여 부서원에게 암호화하여 관리하도록 요구할 수 있다.
93. **암호화 적용**
94. 파일형태의 정보자산은 파일 자체를 회사의 암호화 솔루션을 이용하여 보안등급에 따라 비밀 이상인 경우 암호화하여야 한다.
95. 정보전달을 위한 암호화는 패스워드 및 키를 통해 암·복호화를 한다.
96. **안전한 키 관리**

내용 키 유효기간 설정은 다음과 같은 원칙을 적용해야 한다.

1. 정보보호 관리자는 키의 유효 기간을 결정하며, 특별한 사유가 발생한 경우는 유효기간을 변경할 수 있다. 암호 키 유효기간이란, 사용자 또는 관리자가 특정한 키를 사용할 수 있도록 허용된 기간 또는 특정 시스템에 주어진 키의 유효성을 유지하는 기간이다.
2. 키의 유효기간을 설정할 때는 키 노출을 야기하는 위험 요소와 키 노출에 따른 비용 등을 고려하여야 한다.
3. 공개키 암호방식의 개인키와 공개키 각각은 별개의 키 유효기간을 가진다.
4. 암호화와 복호화에 동일한 키를 사용하는 대칭 암호화 방식에서의 암호 키의 유효기간은 암호화가 적용되는 시기부터 해당 암호문을 복호화하는 시기까지이다.
5. 키 유형별 유효기간은 다음을 따른다.

|  |  |
| --- | --- |
| **키유형** | **유효기간** |
| 암호 키 | 2년 이하 |
| 키 암호 | 2년 이하 |
| 마스터 키 | 약 1년 |
| 암호 키 분배 개인키 (전송방식) | 2년 이하 |
| 암호 키 분배 공개키 (전송방식) | 1 ~ 2 년 |
| 암호 키 분배 개인키 (동의방식) | 1 ~ 2 년 |
| 암호 키 분배 공개키 (동의방식) | 1 ~ 2 년 |

1. 암호키는 다음과 같이 백업하는 것을 원칙으로 한다.
2. 암호 키의 유실에 대한 신속한 대응을 위하여 파일의 형태로 된 키를 분배 시에는 정보보호 관리자가 별도의 매체에 백업을 실시하며, 암호키는 별도로 저장하여 캐비닛에 보관하도록 한다.
3. **개인정보보호관리**
4. **개인정보 관리**
5. **개인정보 관리계획(내부관리계획) 수립 및 이행**

개인정보보호 주관부서는 관련 법률에 따라 다음 사항을 포함하는 개인정보 관리계획을 연1회 수립하고, 개인정보 관리책임자의 승인을 득해야 한다.

1. 개인정보 관리책임자의 지정 등 개인정보보호 조직 구성 및 운영
2. 개인정보 관리책임자와 개인정보취급자의 역할 및 책임
3. 개인정보 내부관리계획의 수립/승인 및 공표
4. 개인정보의 기술적․관리적 보호조치 이행 및 점검
5. 그 밖에 개인정보보호를 위해 필요한 사항
6. **개인정보의 식별 및 취급자의 지정**
7. 개인정보 주관부서는 회사에서 수집∙이용하는 개인정보를 식별하여 관리하여야 하며, 업무상 해당 개인정보를 취급하거나 개인정보처리시스템의 접근권한을 보유하고 있는 임직원을 개인정보취급자를 지정하여 관리∙감독하여야 한다.
8. 개인정보보호 주관부서는 개인정보 처리자, 개인정보 처리시스템을 정기적으로 식별하고 목록을 최신화하여 관리하며, 개인정보 흐름도를 연 1회 검토하여 최신화하여야 한다.
9. **개인정보 처리 방침의 작성 및 관리**

개인정보보호 주관부서는 개인정보보호취급방침을 수립하여 공개하여야 하며, 개인정보취급방침은 다음 각 사항을 포함하여야 한다.

1. 개인정보의 수집∙이용 목적
2. 수집하는 개인정보의 항목 및 동의가 명시된 수집방법
3. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용목적과 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용기간, 개인정보의 파기절차 및 파기방법(개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
5. 개인정보 처리위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 포함한다)
6. 이용자 및 법정대리인의 권리와 그 행사방법
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
8. 개인정보 관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처
9. **개인정보 수집관리**
10. **개인정보의 수집 및 동의**
11. 개인정보를 수집할 경우에는 정보주체에게 동의를 받아야 한다. 단, 다음 각 사항의 어느 하나에 해당하는 경우에는 예외로 할 수 있다.
12. 법률에서 개인정보를 수집∙이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우
13. 서비스 제공에 대한 계약을 체결하고 이행하기 위하여 필요한 개인정보로서, 경제적∙기술적 사유로 통상의 동의를 받는 것이 뚜렷하게 곤란한 경우
14. 만 14세 미만의 개인정보는 수집할 수 없다. 단, 업무상 필요할 경우에는, 개인정보보호 주관부서와 협의하여 법정대리인에게 필요한 사항을 고지하고 만 14세 미만의 정보주체의 동의를 받아야 한다.
15. **수집시 최소화의 원칙**
16. 개인정보를 수집할 경우에는 서비스 제공에 필요한 최소한의 개인정보만 수집하여야 하며, 그 외의 정보를 수집할 경우에는 정보주체가 선택할 수 있는 방법을 제공하여야 한다.
17. 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.
18. **중요정보의 수집제한**

개인정보 중 사상, 신념, 과거의 병력(病歷) 등 정보주체의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보는 정보주체의 동의를 받거나 법률에 의하는 경우에만 수집할 수 있다.

1. **고유식별정보의 수집제한**

회사는 법률에서 고유식별정보 수집∙이용을 허용하는 경우에만 수집할 수 있으며, 별도의 동의를 받아야 한다.

1. **개인정보 수집시 고지**

정보주체의 개인정보 수집 시 다음 사항을 고지하고 동의를 받아야 하며, 수집동의 기록이 보관되어야 한다. 다음 사항이 변경된 경우에도 동일하다.

1. 개인정보의 수집 · 이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유 · 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
5. **동의를 받는 방법**
6. 개인정보 수집∙이용, 고유식별정보 수집∙이용, 개인정보 처리위탁, 개인정보 제공에 대하여 각각 구분하여 동의를 받아야 하며, 이에 동의를 거부한다는 이유로 서비스 제공을 거부할 수 없다.
7. 동의를 받을 때에는 필수 정보와 선택 정보를 구분하여 각각 동의를 받아야 하며, 동의 기록은 보관하여야 한다.
8. **개인정보 이용 관리**
9. **개인정보 이용의 제한**

개인정보는 수집한 목적 내에서만 이용하여야 하며, 목적 외 이용 또는 제3자 제공할 경우에는 정보주체로부터 추가적인 동의를 받아야 한다.

1. **개인정보의 위탁**
2. 개인정보를 제3자에게 취급 위탁하는 경우에는, 다음 각 사항을 정보주체에게 고지하고 동의받아야 한다. 각 사항을 변경하는 경우에도 변경 사항에 대해 정보주체에게 고지하고 동의 받아야 한다.
3. 개인정보 처리위탁을 받는 자
4. 개인정보 처리위탁 업무 내용
5. 서비스 제공에 관한 계약을 이행하기 위하여 필요한 경우로서, 개인정보취급방침을 통하여 수탁자 및 개인정보 처리위탁 업무 내용을 정보주체에게 고지한 경우에는 개인정보 처리위탁에 따른 고지 및 동의를 받지 않아도 된다. 고지의 내용이 변경되는 경우 또한 같다.
6. 개인정보의 취급을 위탁하는 경우 자체 교육 및 관리감독 결과를 반기 1회 수령하여야 한다.
7. **개인정보의 제3자 제공**
8. 개인정보를 협력사, 제휴사 등 제3자에게 제공하는 경우에는, 서비스 제공을 위한 요금정산 또는 법률에 규정이 있는 경우 외에는 다음 각 사항을 정보주체에게 고지하고 동의 받아야 한다. 각 사항을 변경하는 경우에도 변경 사항에 대해 정보주체에게 고지하여야 한다.
9. 개인정보를 제공받는 자 및 개인정보 이용 목적
10. 제공하는 개인정보의 항목 및 개인정보 보유∙이용 기간
11. 개인정보를 제3자에게 제공하는 경우에는, 안전한 절차를 통하여 최소한의 개인정보만 제공하여야 한다.
12. 개인정보를 제공받은 경우에는, 제공받은 목적 내에서만 이용하여야 제3자에게 제공할 수 없다. 다만, 정보주체의 동의가 있거나 법률의 규정이 있는 경우에는 예외로 한다.
13. **개인정보 위탁시 보안요구사항**

개인정보를 제3자에게 위탁하는 경우에는, 계약서에 다음 각 사항을 포함하여야 한다.

1. 개인정보 처리위탁 업무의 목적 및 범위
2. 위탁업무 수행 목적 외 개인정보의 처리 제한에 관한 사항
3. 개인정보의 기술적∙관리적 보호조치에 관한 사항
4. 개인정보의 관리 현황 점검 및 감독에 관한 사항
5. 수탁자의 의무 준수 위반 시 법적 책임 및 손해배상 등 책임에 관한 사항
6. 기타 개인정보 처리위탁에 필요한 사항
7. **개인정보의 관리감독**

개인정보 관리책임자는 개인정보 처리업무를 수탁자에게 위탁하는 경우에는, 개인정보보호 교육, 개인정보 처리 현황 및 실태, 목적 외 이용∙제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 관리∙감독하여야 한다.

1. **개인정보 파기 관리**
2. **파기 시점**
3. 개인정보 관리책임자는 개인정보의 수집∙이용 목적을 달성한 개인정보는 파기하여야 한다. 단, 법률에 의하여 일부 또는 전부를 보존하여야 하는 경우에는 예외로 한다.
4. 개인정보의 수집∙이용 목적 달성 후에도 법률에 의하여 개인정보의 일부 또는 전부를 보유하는 경우에는, 최소한의 개인정보만 보유하여야 하며 보유근거, 보유목적, 보유기간 및 보유항목을 고지하여야 한다.
5. **개인정보 파기 방법**

개인정보를 파기할 경우에는, 다음 각 사항의 어느 하나의 방법으로 복구 또는 재생하지 못하도록 파기하여야 한다.

1. 개인정보가 포함 된 전자적 파일 형태의 경우에는 복구가 불가능하도록 완전 삭제한다.
2. 단, 전자상거래에 관한 기록은 추후 분쟁의 소지가 있으므로, 비식별화 조치를 하여 회사 영업 종료 시까지 보관한다
3. 개인정보가 인쇄, 기록된 문서는 파쇄기로 파쇄하거나 소각한다.
4. **휴면 이용자 정보 파기**

1년 동안 회사의 서비스를 이용하지 않은 정보주체의 개인정보는 1년의 기간 경과 후 파기하거나 다른 개인정보와 별도로 분리하여 저장∙관리하여야 한다. 단, 다음 각 사항의 경우에는 해당 기간으로 한다.

1. 다른 법률에서 별도의 기간을 정하는 경우에는 해당 법률 기간
2. 정보주체가 기간을 다르게 정한 경우에는 해당 기간
3. **정보주체의 권리 보호**
4. **개인정보의 열람**
5. 정보주체로부터 개인정보의 열람이나 제공을 요구 받았을 때에는 개인정보의 열람 또는 제공에 대한 필요한 조치를 하여야 한다.
6. 정보주체가 해당 개인정보의 오류에 대한 정정을 요구할 경우에는, 오류를 정정하거나 오류를 정정하지 못하는 사유를 알리는 등 필요한 조치를 하여야 한다. 단, 법률에 의하여 개인정보의 제공을 요청 받은 경우 외에는 필요한 조치를 할 때까지는 해당 개인정보를 이용하거나 제공할 수 없다.
7. **동의의 철회**

정보주체로부터 개인정보 수집·이용·제공 등의 동의에 대한 철회를 요청 받았을 경우에는 필요한 조치를 하여한다. 단, 법률에 의해 동의철회 후에도 개인정보를 보관하는 경우에는 적절한 보호조치를 취하여야 한다.

1. **개인정보 이용내역의 통지**

정보주체로부터 수집한 개인정보 이용내역에 대해 요청받을 경우 다음 각 사항의 내역을 통지하여야 한다.

1. 개인정보의 수집∙이용 목적 및 수집한 개인정보의 항목
2. 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목
3. 개인정보 처리 위탁을 받은 자 및 그 취급위탁을 하는 업무의 내용
4. **개인정보 유출 시 신고**

개인정보의 분실·도난·유출(이하 '유출 등'이라 한다) 시에는 다음 각 사항을 10일 이내에정보주체에게 알리고 지정된 기관(한국인터넷진흥원)에 즉시 신고하여야 한다. 단, 정보주체의 연락처를 알 수 없는 경우에는 홈페이지에 30일 이상 게시하여야 한다.

1. 유출 등이 된 개인정보 항목
2. 유출 시점
3. 정보주체가 취할 수 있는 조치
4. 회사의 대응 조치
5. 정보주체가 상담 등을 접수할 수 있는 부서 및 연락처
6. **개인정보의 안전성 확보조치**
7. 회사는 매년 내부관리계획을 수립하고 최고책임자의 승인 하에 공표 후, 계획을 시행한다.
8. 회사는 개인정보관리에 대해 안전성 확보조치 기준에 의거하여 개인정보의 관리적, 물리적, 기술적 조치를 취한다.
9. **영상정보관리**
10. **영상정보관리**

영상정보처리기기 운영ㆍ관리 방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

1. 영상정보처리기기 운영자는 정보주체가 영상정보처리기기가 설치․운영 중임을 쉽게 알아볼 수 있도록 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다.
2. 설치목적 및 장소
3. 촬영범위 및 시간
4. 관리책임자의 성명 또는 직책 및 연락처
5. 영상정보처리기기 설치ㆍ운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처
6. 제1항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 영상정보처리기기 운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.
7. 영상정보처리기기 운영자는 수집한 개인영상정보를 사전에 명시한 보관 기간이 만료한 때에는 지체 없이 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.
8. 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.
9. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
10. 전자기적 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제
11. 영상정보처리기기 운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 한다.
12. 파기하는 개인영상정보 파일의 명칭
13. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 대한 확인 시기)
14. 개인영상정보 파기 담당자
15. **감사**
16. **계획 수립**

보안감사조직은 보안감사를 실시하기 위해 연간 보안감사계획을 수립하고 이에 따라 보안감사를 실시한다

1. **조직**

보안감사는 정보보호 관리자와 정보보호 관리자가 지정한 정보보호 담당자가 수행하는 것을 원칙으로 하며 추가지원이 필요한 경우 내∙외부 전문가를 포함할 수 있다.

1. **방법**
2. 보안감사인은 보안감사 계획에 따라 보안감사를 수행하여야 한다.
3. 보안감사인은 업무 중단의 위험을 최소화할 수 있도록 업무 환경을 고려하여 보안감사를 수행하여야 한다.
4. **사후 관리**

감사 결과는 정보보호 최고책임자에게 보고하여야 하며, 감사 지적사항에 대해서 적절한 시정 조치 및 시정조치에 대하여 추후 확인하여야 한다.

1. **사고관리**
2. **보안사고 예방 활동**
3. 정보보호 담당자는 보안사고 발생 가능성을 사전에 점검하고 보안사고를 감지할 수 있는 대책을 마련하여야 한다.
4. 정보보호 담당자는 보안사고 관련 정보를 사내 게시판 등을 이용하여 임직원들에게 공지하여야 한다.
5. 정보보호 관리자는 보안사고 발생 시 신속한 대응을 위하여 절차를 마련하여야 한다.
6. **보안사고 대응관리**
7. 보안사고 발생시 선 보고 후 조치를 원칙으로 한다. 다만, 긴급 상황일 경우에는 선 조치 후 보고할 수 있다.
8. 모든 이상 징후에 대해서는 분석을 실시한다. 정보보호 관리자는 이를 총괄한다.
9. 보안사고 발생이 의심되거나 실제 사고가 발생했을 경우, 법적 증거 확보를 위하여 시스템에 대한 보안 공격 시도나 침해 사실을 판단할 수 있는 로그, 보안사고 발생 흔적 및 파일이나 기타 정보 등을 수집하여 보관한다.
10. 모든 보안사고 관련 분석, 조치, 보고에 대한 사항은 “보안사고 대응 보고서”에 작성한다.
11. **보안사고 결과보고 및 복구**
12. 정보보호 담당자는 보안사고 대응반의 각 관련 부서에서 작성한 “보안사고 조치 보고서”를 취합하여 그 결과를 정보보호 관리자에게 보고하며, 정보보호 관리자는 보안사고에 대하여 정보보호 최고책임자에게 사고 경과와 조치사항을 보고한다.
13. 보안사고가 발생한 IT 인프라는 네트워크에서 절체하여 내/외부의 접근을 차단하며 동일 시스템 및 관련 시스템에 대하여 최신 보안패치 설치, 패스워드 변경, 불필요한 서비스 중지 등의 보안 대책을 적용하며, 정보보호 관리자는 해당 사항을 점검 및 확인한다
14. **사후 관리**
15. 정보보호 관리자는 유사한 사고의 재발 방지를 위하여, 관련 정책 및 지침의 개정, 정보보호시스템 도입, 유관기관 협조체계 구축 등 효과적인 재발방지 대책을 수립하여야 한다.
16. 정보보호 관리자는 수립된 재발방지 대책을 정보보호위원회에 보고하여 동일 또는 유사 사고의 재발에 대비하여야 하며 보안사고의 대응 및 복구가 완료되었음을 확인하여야 한다.
17. 정보보호 담당자는 보안사고 관련된 기록을 대외비 이상 등급으로 분류하고, 이를 보존, 관리하여야 한다.
18. 법적 또는 규정 상 보안사고 관련하여 대외 기관의 협조 요청이 있는 경우, 대외협력 관련부서는 정보보호 관리자와 협의 후 대응하여야 한다.

끝.

**부 칙**

**(시행일)** 이 정책은 2018. 10. 05 부터 시행한다.