DOC-POL-005

**인프라 운영보안 지침서**

개정번호 : 1.00

**㈜1 Shop**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **개 정 이 력** | | | | | | |
| **문서명** | | 인프라 운영보안 지침서 | | | | |
| **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 개 요 6](#_Toc381275457)

[제1조 목적 6](#_Toc381275458)

[제2조 적용 대상 6](#_Toc381275459)

[제2장 Infra 일반 관리 6](#_Toc381275460)

[제1절 Infra 공통 관리 6](#_Toc381275461)

[제3조 보안성 검토 6](#_Toc381275462)

[제4조 접근 통제 8](#_Toc381275463)

[제5조 계정 관리 9](#_Toc381275464)

[제6조 인증 관리 9](#_Toc381275465)

[제7조 비밀번호 관리 11](#_Toc381275466)

[제8조 암호화 12](#_Toc381275467)

[제9조 보안설정 관리 12](#_Toc381275468)

[제10조 보안패치 관리 12](#_Toc381275469)

[제11조 로그 관리 13](#_Toc381275470)

[제12조 변경 관리 15](#_Toc381275471)

[제13조 백업 및 복구 15](#_Toc381275472)

[제14조 취약성 점검 16](#_Toc381275473)

[제15조 폐기 및 재사용 16](#_Toc381275474)

[제3장 시스템 별 보안 17](#_Toc381275475)

[제1절 서버보안 17](#_Toc381275476)

[제16조 도입 17](#_Toc381275477)

[제17조 설치 17](#_Toc381275478)

[제18조 로깅 및 모니터링 17](#_Toc381275479)

[제2절 웹 서버 보안 18](#_Toc381275480)

[제19조 설치 및 운영 18](#_Toc381275481)

[제3절 네트워크 보안 19](#_Toc381275482)

[제20조 네트워크 구성 관리 19](#_Toc381275483)

[제21조 도입 및 설치 22](#_Toc381275484)

[제22조 네트워크 분리 23](#_Toc381275485)

[제23조 무선 네트워크 관리 24](#_Toc381275486)

[제4절 DB 보안 24](#_Toc381275487)

[제24조 도입 및 설치 24](#_Toc381275488)

[제25조 DB 암호화 25](#_Toc381275489)

[제5절 응용 프로그램 보안 26](#_Toc381275490)

[제26조 관리자 접근 관리 26](#_Toc381275491)

[제6절 정보보호시스템 보안 26](#_Toc381275492)

[제27조 정보보호시스템 구성관리 26](#_Toc381275493)

[제28조 도입 27](#_Toc381275494)

[제29조 시스템 운영 27](#_Toc381275495)

[제7절 개인정보처리시스템 보안 27](#_Toc381275496)

[제30조 개인정보 관리 28](#_Toc381275497)

[제4장 서비스 연속성 관리 29](#_Toc381275498)

[제31조 장애관리 29](#_Toc381275499)

[제32조 가용성 관리 29](#_Toc381275500)

[제33조 업무연속성 계획 30](#_Toc381275501)

[제34조 유지보수 관리 31](#_Toc381275502)

[제5장 외주인력 보안 31](#_Toc381275503)

[제35조 보안 통제 31](#_Toc381275504)

[제6장 출입통제 관리 31](#_Toc381275505)

[제1절 일반 관리 32](#_Toc381275506)

[제36조 원칙 32](#_Toc381275507)

[제37조 출입권한 관리 32](#_Toc381275508)

[제2절 통제구역의 관리 33](#_Toc381275509)

[제38조 통제 구역 설정 33](#_Toc381275510)

[제39조 출입 통제 34](#_Toc381275511)

[제40조 통제구역 내 작업 35](#_Toc381275512)

[제41조 배달 및 하역 구역의 분리 35](#_Toc381275513)

[제3절 IT 인프라 보호 36](#_Toc381275514)

[제42조 보호대책 36](#_Toc381275515)

[제43조 케이블 보호 36](#_Toc381275516)

[제44조 인프라 반출 37](#_Toc381275517)

개 요

1. 목적

본 지침은 ㈜1 Shop(이하 ‘회사’라고 한다)의 서버, 네트워크, DB, 어플리케이션 및 주변장치 등의 시스템 자산이 유출, 손상, 파괴 등 일련의 불법적 행위와 보안사고로부터 안전하게 운영될 수 있도록 그 업무기준과 절차를 정함에 그 목적이 있다.

1. 적용 대상

본 지침은 회사에서 규정하고 있는 IT 인프라 자산에 적용되며 아래 내용을 포함한다.

1. 서버보안
2. 웹서버 보안
3. 네트워크 보안
4. DB 보안
5. 응용프로그램 보안
6. 정보보호시스템 보안
7. 개인정보처리시스템 보안

Infra 일반 관리

1. Infra 공통 관리
2. 보안성 검토
3. 업무시스템 및 개인정보 처리시스템에 대한 보안성 확보가 요구되는 경우 정보보호 관리자에게 요청하여 보안성 심의를 받아야 한다.
4. 다음과 같이 중요한 사안에 대해서는 정보보호 최고책임자의 보안성 심의를 받아야 한다.
5. 내부 시스템이 외부 기관의 시스템과 데이터 전송을 위하여 최초로 연동되는 경우
6. 내부 시스템이 외부 기관의 시스템과 연동 후 추가로 개인정보를 송수신하는 경우
7. 외부 네트워크 및 DMZ를 통해 외부로 공개되는 시스템(공개용 웹서버 포함) 및 네트워크 장비를 설치하는 경우
8. 협력업체, 외부 유지보수 업체 등이 외부 네트워크로부터 원격접속을 통해서 서비스를 제공하는 경우
9. 개인정보 등 중요한 정보를 저장 · 관리하는 시스템을 도입하는 경우
10. 보안장비 및 암호 프로그램 등 정보보호 시스템을 도입하는 경우
11. 시스템 OS 또는 소프트웨어 등에서 제공하거나, 응용 프로그램 개발을 통해 제작된 보안 유틸리티를 설치 · 실행하고자 하는 경우
12. IT개발 및 운영업무의 일부 또는 전체를 외부에 용역 · 의뢰하는 경우
13. IT운영 · 개발 업무 수행 시 보안에 중대한 영향이 있을 것으로 판단되는 경우
14. 기타 정보보호 최고책임자가 심의한 사항에 대하여 변경이 필요한 경우
15. 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.
16. 보안성 심의 절차는 “보안성 심의 프로세스”를 따른다.
17. 정보보호 최고책임자는 특별한 사유가 없는 한 보안성 심의가 필요한 경우 지체없이 심의를 진행하여야 한다.
18. 정보보호 최고책임자는 심의 결과에 추가적인 보안대책을 마련하도록 요청할 수 있다.
19. 정보보호 최고책임자는 검토자료가 불충분한 경우 추가자료를 요청할 수 있다.
20. 접근 통제
21. 접근통제가 요구되는 업무가 정의되어 있고, 이 업무에 대한 접근통제 방법과 범위 등을 문서화하고 있어야 한다.
22. 접근통제 정책은 데이터, 프로그램, 주요시스템, 네트워크 등의 접근통제 대상을 명확하게 식별할 수 있도록 정의하여야 한다. 그리고 정보보호 관리자는 접근통제 및 권한관리 현황을 “접근통제 및 권한관리 대장”로 관리하여야 한다.
23. 접근통제 정책에는 보안요구사항, 데이터 및 서비스 접근시의 법적, 계약적 제한, 분산 네트워크상의 접근권한 관리 등 사업 관련 법적, 계약적 요건이 접근통제에 반영하여야 한다.
24. 항상 적용되는 접근통제 규칙과 일정기간이나 또는 선택적으로 존재하는 접근통제 규칙이 구분되어 있어야 한다.
25. 보안상 중요한 접근통제 규칙의 경우, 관리자의 승인을 거쳐서만 설정 또는 변경하도록 하여야 한다.
26. 접근통제 기능 또는 소프트웨어를 포함하여 접근통제 정책 및 절차를 수행할 수 있는 방법이 존재하고, 이에 따라 적절히 운영하여야 한다.
27. 정보보호 담당자는 정보시스템의 접근을 모니터링하여 정책과의 일치성을 반기 1회 검토하여야 한다,
28. 정보보호 관리자는 접근통제 정책이 주변환경의 변화 또는 사업 내용이나 정보시스템 환경의 변화에 따라 적정한지를 연 1회 검토하여야 한다.
29. 정보보호 관리자는 사용자 접근권한에 대해 연 2회 검토하고 재승인 및 보고를 시행하여야 한다.
30. 계정 관리
31. 기술보안 담당자는 사용자계정 생성 시 각 부서장의 승인 여부를 확인하여 사용자계정을 생성하여야 한다. 또한 사용자계정 생성 후 “정보시스템 계정 관리 대장”에 따라 기록 및 관리하여야 한다.
32. 정보보호 담당자는 사용자의 부서변경, 퇴직, 휴직 등의 상태 변동 사항 발생 시 시스템에 반영하여야 한다.
33. 정보보호 관리자는 월 1회 정보시스템에 대해 미승인 사용자계정의 존재, 퇴사자계정의 활성화 여부를 점검하여야 한다.
34. 정보보호 담당자는 정보시스템 도입 시 초기설정 계정, Guest계정 등 불필요한 계정에 대해 삭제하거나, 사용중지로 설정하여야 한다.
35. 정보보호 관리자는 각 부서장과 협의하여 정보시스템 관리자계정의 권한을 제한할 수 있다.
36. 테스트시스템의 사용자계정 및 관리자계정은 실제시스템과 동일하게 관리하여야 한다.
37. 정보보호 관리자는 업무위탁 외주인력 등에게 정보시스템 사용자계정을 부여하는 경우 해당업무가 종료되는 경우 지체없이 계정을 삭제하여야 한다.
38. 정보보호 관리자는 정보시스템 관리자 계정을 장애복구 또는 점검을 위하여 외부 유지보수자에게 일시 공개한 경우 작업 종료 후 부여된 계정의 비밀번호를 변경하여야 한다.
39. 인프라 시스템에 직접 접속 가능한 계정을 특수권한으로 설정 한다.
40. 인증 관리
41. 정보보호 관리자는 정보시스템 도입 시 사용자 인증절차에 대해 검토하여야 한다.
42. 정보보호 관리자는 주요시스템, DB, 어플리케이션 등에 대해 다음 각 호의 접속 제한절차를 결정할 수 있다.
43. 비밀번호 자릿수 및 사용가능문자 제한
44. 생년월일, 주민등록번호, 전화번호 등 인식하기 쉬운 비밀번호 등록 제한
45. 최근 사용한 비밀번호 등록 제한
46. 계정명과 동일한 비밀번호 등록 제한
47. QWER, 1234 등 컴퓨터자판의 연속적인 자판 배열에 의한 비밀번호 등록 제한
48. 비밀번호 변경주기
49. 연속적인 비밀번호 오류 입력에 대한 사용자계정 회수
50. 비밀번호 마스킹 처리
51. 일정기간 사용하지 않는 사용자계정 회수
52. 모든 정보시스템에는 비밀번호가 없는 계정을 허용할 수 없다.
53. 정보시스템 접속인증을 위해 사용하는 모든 비밀번호는 평문으로 조회가 불가능 하도록 DB저장방향으로 일방향 암호화하여야 하며, 어떠한 경우라도 복호화 할 수 없다.
54. 연속적인 비밀번호 오류 입력으로 사용자계정이 회수된 사용자 및 장기 휴직, 출장 등으로 인해 비밀번호를 분실한 사용자는 정보보호 최고책임자의 사용자계정 재사용 승인을 받아야 한다.
55. 사용자계정 재사용 승인에 따라 부여되는 초기화 비밀번호는 반드시 임의의 문자로 제공되어야 한다.
56. 초기화 비밀번호는 최초 접속 시 다른 비밀번호로 변경하여야 한다.
57. 정보보호 관리자는 사용자에게 시스템과 패스워드 관리책임이 있음을 주지시켜야 한다.
58. 시스템 관리자, 시스템 운영자, 공급업체 기술자, 유지보수 요원 등 특권 사용자는 명시적으로 제한하여야 한다.
59. 비밀번호 관리
60. 시스템의 관리를 위한 패스워드 사용시에는 타인이 추측하기 어려운 패스워드를 사용하여야 하며, 다음과 같은 조치를 하여야 한다.
61. 패스워드는 문자, 숫자, 특수문자를 혼용하여 8자리 이상(2종류 10자리, 3종류 8자리)
62. 연속 숫자, 생일, 전화번호, 아이디 등 추측하기 쉬운 개인 신상정보를 활용한 취약 패스워드 사용 제한
63. 초기/임시 패스워드 발급의 경우 최초 로그인 시 변경
64. 주기적인 패스워드 변경 유도(반기 1회)
65. 패스워드 처리(입력, 변경) 시 마스킹 처리
66. 패스워드 분실 및 도난 시 안전한 재발급 절차(본인인증 등)를 수립하여 재발급을 통한 도용 방지(임시 패스워드 발급 시 안전한 전송 및 로그인 후 변경)
67. 안전한 패스워드 작성규칙, 추측하기 쉬운 패스워드 사용 제한, 발급받은 초기/임시 패스워드 최초 로그인 시 변경, 패스워드 주기적 변경 유도, 패스워드 입력 시 마스킹 처리 등의 규칙을 기술적 기능으로 반영하여야 한다.
68. 응용 프로그램의 경우, 패스워드는 별도의 프로그램을 통하여 암호화되어 저장하도록 개발 시에 고려하여야 하며, 업무성격에 따라 자체 암호화 알고리즘을 적용할 수도 있다..
69. 암호화
70. 업무위탁회사, 제휴사, 고객사 등 외부기관과 파일형태로 정보를 제공하는 개인정보는 암호화하여야 한다.
71. 보안등급에 따라 비밀 이상의 보안등급을 갖는 정보자산은 안전한 암호화 알고리즘을 사용하여 암호화 후 저장 · 관리하여야 한다.
72. 암호화 대상 정보는 전용선, 인터넷 등 통신망의 보안 취약성에 상관없이 암호화하여야 한다.
73. 이용자, 사용자의 패스워드, 결재정보 및 임직원 PC의 개인정보포함 문서는 암호화하여야 한다.
74. 제1항 ~ 제3항에도 불구하고 정보보호최고책임자의 승인을 받은 경우에는 암호화 대상에서 예외로 인정할 수 있다.
75. 정보보호 최고책임자는 회사 내부 또는 외부에서 암호화가 필요하다고 판단되는 정보, 통신구간, DB 테이블 등에 대해 암호화 관리를 요구할 수 있다.
76. 각 부서장은 해당 부서에서 관리하고 있는 주요 정보에 대하여 부서원에게 암호화하여 관리하도록 요구할 수 있다.
77. 보안설정 관리
78. 기술보안 담당자는 시스템 설치 시 서비스의 안정적 운영 및 침해사고 위험을 최소화 하기 위해 보안 설정을 적용하여야 한다.
79. 기술보안 담당자 외 타인의 보안설정 변경을 금지하여야 하며, 서비스와의 충돌 등으로 인해 적용이 불가능한 보안설정 항목은 운영자가 정보보호 주관부서에 통보하여 별도 관리방안을 적용하여야 한다.
80. 기술보안 담당자는 정보보호 주관 부서의 서버 보안설정 적용여부 등에 대한 보안성 검토 시 협조하여야 한다.
81. 보안패치 관리
82. 정보보호 관리자는 시스템공급업체의 보안관련 패치나 권고안의 발생 여부를 지속적으로 모니터링 하여야 하며, 새로운 버전의 보안패치를 적용하여야 한다.
83. 정보보호 관리자는 성능향상 및 보안패치 적용 전에 테스트 시스템에서 사전검증 후 실운영시스템에 적용하여야 한다.
84. 기술보안 담당자는 보안패치 적용 전에 주요정보를 백업하고, 보안패치를 적용하여야 한다.
85. 시스템에 대한 긴급성을 요하는 중요 보안패치는 즉시 적용하는 것을 원칙으로 한다.
86. 로그 관리
87. 정보보호 관리자는 IT 인프라(정보시스템, 네트워크 장비, DB, 어플리케이션)의 특성 등을 고려하여 로그항목 및 관리체계를 수립하여야 하며, 연 1회 관리항목을 검토·보완하여야 한다.
88. 기술보안 담당자는 다음과 같은 로그를 반기 1회 검토하여 이상 유무를 확인하고 로그는 1년간 보관하여야 한다.
89. 서버 담당자
90. 정보시스템에 접근한 사용자계정
91. 접속일시
92. 사용내역 정보
93. 네트워크 담당자   
    본 회사는 해당 없음
94. DB 담당자
95. 사용자의 접속시각 및 접속종료까지의 시간
96. 사용자의 Table 접근
97. DB에 연결된 사용자의 수
98. Table 접근에 실패한 접근 시도
99. System Table 접근
100. 새로운 DB 객체의 생성
101. 데이터 조작 정보
102. 어플리케이션 담당자
103. 사용자계정
104. 사용일시
105. 변경 또는 조회 내용
106. 접속방법
107. 기술보안 담당자는 로그 기록을 검토하여 침입 또는 시도 오남용의 흔적 등 문제점이 있을 경우 “DOC-POL-002\_정보보호 및 개인정보보호 업무지침”에 따라 조치하여야 한다.
108. 모든 임직원은 업무수행 중 다음 각 호의 이상로그를 발견한 경우 정보보호 최고책임자 및 정보보호 관리자에게 알리고, 정보보호 관리자는 해당로그를 검토 · 분석한 후 유지보수 업체와 협의 후에 안전하게 관리하여야 한다.
109. 비정상적 패턴의 로그인 실패
110. 시스템 파일에 대한 접근 실패
111. 정보보안과 관련되는 작업 수행에 대한 실패
112. 관리자 특권이 있는 파일 또는 서비스에 대한 비인가 사용 시도
113. 비인가된 파일, 자원 또는 서비스의 사용 시도
114. 기타 보안과 관련된 비정상적 행위
115. 정보보호 관리자는 이상로그 분석결과 보안사고가 발생하였거나, 발생할 가능성이 있는 경우 “DOC-POL-002\_정보보호 및 개인정보보호 업무지침”에 따라 조치하여야 한다.
116. 변경 관리
117. 허가된 사용자만이 변경을 요청할 수 있다.
118. 변경의 수행 전에 상세한 변경내역을 문서로 승인하여야 한다.
119. 변경요청에 대한 기록을 검토하여 해결 여부를 확인하고 필요한 조치를 취하는 절차가 있어야 한다.
120. 변경 사항에 관련된 프로그램 및 매뉴얼은 해당 변경을 반영하여 변경되어야 한다.
121. 변경 완료 후 일정 기간이 지나 사용자의 반응을 확인하고 문제가 발생된 것이 없는지 확인하는 절차가 있어야 한다.
122. 변경 및 사용방법의 변동 사항은 관련 사용자 및 운영자에게 적시에 교육되어야 한다.
123. 변경에 따른 개인정보에 대한 새로운 위험 발생 여부와 보호 요건을 확인하기 위하여 변경의 규모와 적절한 보안성 심의를 시행하고 필요한 경우 대책을 개발하여야 한다.
124. 정보시스템 관련 자산의 변경 관리 경우 보안성 심의를 시행하여야 한다.
125. 백업 및 복구
126. 정보보호 관리자는 시스템 장애, 데이터 파손 등으로 인한 피해를 최소화하고, 조속한 복구를 위하여 시스템 가동 및 복구에 필요한 데이터의 백업계획을 수립하여 운영하여야 한다.
127. 기술보안 담당자는 백업계획에 따라 정기 또는 필요시에 백업을 실시하여야 한다.
128. 기술보안 담당자는 백업매체에 작업일, 데이터내역 등 관련정보를 표시하고, 백업매체의 위치와 내용을 목록화하여 관리하여야 한다.
129. 정보보호 관리자는 화재 및 지진 등의 재해로부터 데이터 유실을 방지하기 위하여 주요데이터의 백업매체를 별도의 지역(금고)에 소산 · 보관하는 계획을 수립하여 운영하여야 한다.
130. 시스템을 외주 관리하는 경우 백업 및 복구 요건을 계약서 또는 SLA에 반영하여야 한다.
131. 취약성 점검
132. 기술보안 담당자는 시스템 자체 보안점검 체크리스트를 작성하여 시스템에 대한 보안점검을 실시하여야 한다.
133. 기술보안 담당자는 연 1회 자체 보안점검을 실시하고 그 결과에 따른 조치를 취해야 한다.
134. 정보보호 최고책임자는 자체 보안점검 결과를 검토하고 그 결과에 따른 조치 사항을 확인하여야 한다.
135. 폐기 및 재사용
136. 정보보호 담당자는 인프라와 저장매체를 분리하고 하위 레벨로 데이터를 모두 삭제한 후 완전 삭제 여부 확인을 위한 자체 보안성 검토를 실시하여야 한다.
137. 검토 결과 문제가 없을 경우 각 기술보안 담당자의 확인을 거쳐 폐기 작업을 진행하고, 자산관리 목록을 갱신하도록 하여야 한다.
138. 정보보호 담당자는 보안성 검토 결과를 “보안성 검토조치 결과서”에 기록하여 연 1회 정보보호 관리자에게 통보하여야 한다.
139. 외부 업체를 이용하여 저장매체를 폐기하거나 재사용할 경우에는 데이터의 완전삭제에 대한 확인을 받아야 한다.
140. 폐기된 시스템는 자산목록에 반영하여 관리하여야 한다.

시스템 별 보안

1. 서버보안
2. 도입
3. 정보보호 관리자는 서버 도입을 위한 계획 및 정책을 수립하여야 한다.
4. 서버 도입을 위한 도입계획 및 정책에는 정보보안과 관련된 가용성, 무결성, 기밀성 측면의 요구사항들을 반영하여야 한다.
5. 새로운 서버의 도입, 업그레이드 시의 승인 기준이 확립되고 구매 계약서 등에 반영되어야 한다.
6. 인수 이전에 시스템 승인 테스트가 수행되어야 하고 기준에 적합할 경우 인수되어야 한다.
7. 설치
8. 정보보호 관리자는 부족한 성능 및 용량으로 인한 실패를 회피하기 위해서 계획을 수립하여야 한다.
9. 현재 장비의 성능 및 용량이 요구되는 사용자의 수준을 만족시켜야 한다.
10. 서버 담당자는 성능 및 용량의 현황과 요구사항을 지속적으로 모니터링하고 기록 및 분석하여 향후 계획 수립에 반영이 되도록 정보보호 관리자를 지원하여야 하며 개선이 필요할 경우 이에 따라 조정하여야 한다.
11. 로깅 및 모니터링
12. 업무처리를 위해 실 데이터를 운영하고 있는 서버를 개발 또는 테스트를 위한 목적으로 사용할 수 없다.
13. 정보보호 최고책임자는 서버에 대해 특정 프로그램의 설치, 특정포트 차단 등을 지정할 수 있다.
14. 업무목적으로 제2항에서 지정한 프로그램의 사용이 필요한 경우 정보보호최고책임자의 승인을 받아야 한다.
15. 서버는 외부전산망에서 관리자의 접속이 불가능하도록 구성되어야 한다. 단, 정보보호최고책임자의 승인이 있는 경우 예외로 한다.
16. 단말기를 통한 서버 접속 시, 최대 15분 동안 사용이 없는 세션은 중단되어야 하며, 서버의 직접 접속도 세션 타임아웃 기능이 있다면 동일한 정책으로 중단되어야 한다.
17. 서버 담당자는 서버의 정확한 기록 관리를 위하여 각 서버의 시간을 동기화해야 한다.
18. 회사 업무의 연속성에 영향을 미치는 회사 소유 서버 장비는 제작사가 권유하는 서비스 권고 사항에 따라 유지 • 보수 계약을 체결하여 관리하여야 한다.
19. 서버 담당자는 서버의 운영절차 및 방안을 수립한다.
20. 정보보호 관리자는 각 서버들이 회사의 보안정책과 운영정책을 이행하고 있는지, 보안위반사항은 없는지 분기 1회 운영기록을 점검하여야 한다.
21. 웹 서버 보안
22. 설치 및 운영
23. 공개용 웹 서버를 내부네트워크와 분리하여 내부네트워크와 외부네트워크 사이(DMZ)에 설치하고 침입차단시스템으로 보호되어야 한다. 단, 침입차단시스템을 직접 운영할 수 없는 경우에는 관련 서비스를 이용할 수 있다.
24. 서버 담당자는 공개용 웹 서버에 접근할 수 있는 사용자계정을 제한하고 불필요한 계정 또는 서비스번호(Port)는 삭제되어야 한다. 공개용 웹 서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험, 개발도구 등의 사용을 제한하여야 한다.
25. 공개용 웹 서버는 실운영시스템과 개발/테스트시스템으로 분리 운영되어야 한다.
26. 공개용 웹서버의 개발/테스트시스템은 실운영시스템과 동일한 네트워크에 위치할 수 없으며, 외부네트워크에 공개될 수 없다.
27. 서버 담당자는 공개용 웹서버에 대해 안전진단프로그램 등을 이용하여 취약성 또는 무결성을 수시 점검하여야 한다. 단, 개인정보 관리책임자가 지정한 홈페이지 보안/운영 담당자에게 해당 점검업무를 이관할 수 있다.
28. 서버 담당자는 공개용 웹서버의 설치 및 운영에 대해 보안위험성 평가를 통해 문제점을 검토하여야 한다.
29. 공개용 웹서버의 관리자 홈페이지는 외부네트워크로의 접속은 차단되어야 한다. 단, 관리가 불가피할 경우 정보보호최고책임자의 승인을 받아야 한다.
30. 공개용 웹서버의 개인정보 및 기밀정보는 파일을 암호화하여 보호하여야 한다.
31. 서버 담당자는 공개 서버의 로그를 분기1회 검토하여 이상 유무를 확인하여야 한다.
32. 서버 담당자는 로그 기록에 침입 또는 침입 시도, 오남용의 흔적 등 문제점이 있을 경우 “DOC-POL-002 정보보호 및 개인정보보호 업무지침”에 따라 조치하여야 한다.
33. 검색도구 등을 통해 공개서버에서 개인정보 노출이 발생할 수 있으므로 이를 방지하기 위한 지침 또는 모니터링이 이루어져야 한다.
34. 네트워크 보안
35. 네트워크 구성 관리
36. IP주소는 다음과 같이 관리한다.
37. 네트워크 담당자는 내부 네트워크의 IP주소를 사설 IP주소로 구성하여야 한다.
38. 회사의 모든 사용자는 회사 내부 네트워크의 IP주소체계를 외부에 유출할 수 없다.
39. 네트워크 담당자는 사용자에게 부여하는 IP주소를 개인별로 부여하고, 기록 ∙ 관리하여야 한다.
40. 회사는 승인을 받지 않은 비인가자에게 IP주소를 부여할 수 없다.
41. 정보보호최고책임자는 IP주소의 원활한 관리를 위해 특정직원 또는 직군에 대한 IP주소 부여를 일괄 승인할 수 있다.
42. 네트워크 담당자는 시스템, 사용자 등이 사용하는 인터넷 이용내역을 IP주소를 포함하여 1년 이상 기록 ∙ 보관하여야 한다.
43. 네트워크 담당자는 정보시스템관리 • 운영자, 개발자 및 업무위탁외부직원 등에 대해 업무 특성 별로 네트워크를 분리하여 관리할 수 있다.
44. 내부 네트워크는 다른 기관의 네트워크와 분리하여야 한다.
45. 인터넷 접속은 다음과 같이 관리한다.
46. 다음을 포함하는 인터넷 접속에 대한 정책을 수립하여야 한다.
47. 인터넷 연결시 네트워크 구성 정책
48. 이메일, 인터넷 사이트의 접속, 소프트웨어 다운로드 및 전송 등의 사용자 접속정책
49. 인터넷 연결은 침입차단시스템에 의해 보호되어야 한다.
50. 침입차단시스템의 정책설정은 회사의 보안정책에 준수되어 설정되어야 한다.
51. 침입차단시스템을 우회하는 모뎀접속, 무선AP, 테더링 등의 우회 인터넷 접속은 금지되어야 하고 이러한 정책이 사용자들에게 공지되어야 한다.
52. 침입차단시스템의 보안설정은 강력하게 수행함으로써 침입차단시스템이 해킹 당할 위험에 대응하여야 한다.
53. 침입차단시스템의 보안정책 변경은 공식적인 절차와 승인에 의해서 이루어져야 한다.
54. 침입차단시스템에는 최신의 패치가 설치됨으로써 과거의 버전에서 보고된 보안위험에 대응하여야 한다.
55. 네트워크 담당자는 침입차단시스템의 로그를 1년 동안 저장하고 분기 1회 점검하여야 한다.
56. 침입차단시스템의 관리기능에 권한이 없는 자가 접근하지 못하도록 접근권한과 접근방법은 강력하게 통제하고 보호하여야 한다.
57. 필요 시 침입차단시스템 외에 VPN을 활용하여 외부와의 원격연결의 보안성을 강화하여야 한다.
58. 개인정보처리시스템 및 개인정보 취급자의 PC를 보호하기 위하여 외부의 침입을 모니터링하고 탐지하는 침입탐지시스템 또는 침입방지시스템을 설치 운용해야 한다.
59. 침입탐지 기록은 수시 또는 주기적으로 검토됨으로써 의심스런 침입사건을 대응해야 한다.
60. 원격 진단포트는 다음과 같이 보호한다.
61. 진단 및 구성포트에 대한 물리적이고 논리적인 접근은 통제되어야 한다.(원격진단 및 구성포트 보호)
62. 전산장비에 유지보수를 위한 원격 진단 포트는 시스템에 대한 비인가된 접근을 허용할 수 있으므로 엄격하게 통제되어야 한다.
63. 유지보수 작업의 필요성 등에 의한 원격 진단 포트의 사용이 있는 경우, 정보보호최고책임자의 승인 및 검토를 받은 후, 작업내역은 기록 • 관리되어야 한다.
64. 이동컴퓨터 및 원격작업은 다음과 같이 관리한다.
65. 이동컴퓨터 보안 정책에 다음과 같은 내용을 포함한다.
66. 이동컴퓨터의 사용
67. 물리적 보호, 접근제어, 암호화, 백업, 바이러스 정책
68. 내부네트워크와의 연결
69. 이동컴퓨터 사용자에 대한 보안교육을 실시하여야 한다.(연 1회)
70. 이동컴퓨터로부터 공공망을 통해 내부 네트워크 접속시의 적절한 식별, 인증, 접근통제 대책(VPN 등 포함)을 수립하여야 한다.
71. 원격작업 시 보안정책과 절차를 수립하여야 한다.
72. 원격작업을 통해 공공망 등을 경유하여 내부 네트워크 접속시의 적절한 식별, 인증, 접근통제 대책(VPN 등 포함)을 수립하여야 한다.
73. 재택근무시 관련 물리적 보안 환경에 대한 지침이 정의되어 있고, 재택근무자가 이 지침을 숙지하며 이에 따른 근무환경을 구성하여야 한다.
74. 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.
75. 원격작업의 기간이 완료되었을 경우 접근권한, 장비 등을 회수하여야 한다.
76. 도입 및 설치
77. 정보보호 최고책임자는 회사 네트워크의 구축 및 변경에 대한 책임이 있다.
78. 내부시스템이 외부기관시스템과 데이터 전송을 위하여 연동하는 경우 전용회선을 사용하여야 한다. 단, 정보보호최고책임자의 보안성 심의를 통해 승인한 경우 예외로 할 수 있다.
79. 네트워크 분리
80. 트래픽의 원활한 분산 및 네트워크 접근통제의 적용을 고려한 계층적인 네트워크를 구성한다.
81. 내부-외부 네트워크 간 기본적인 접근통제를 위해 방화벽을 설치하며, 이때 네트워크 간 우회경로가 없도록 구성한다.
82. 핵심 업무영역으로 지정된 경우에는 기타 시스템 영역과 물리적으로 분리하고 별도의 방화벽을 설치한다.
83. 기타 시스템 영역은 클라이언트, 서버 영역을 기준으로 물리적으로 분리하거나 논리적으로 분리할 수 있다.
84. 내부 네트워크는 외부에서 모니터링 및 유지보수를 위한 관리목적의 원격 접속을 할 수 없다. 단, 특수한 목적에 의해 외부에서 내부 네트워크에 접속이 필요한 경우 정보보호 최고책임자의 승인을 받아야 한다.
85. 외부에서의 내부네트워크 접속은 다음 각 호의 절차를 따라야 한다.
86. 고객의 접속: 고객접속을 위한 서비스 네트워크는 불특정 다수의 접속을 허용한다. 단, 침해사고를 방지하거나, 피해를 최소화하기 위해서 네트워크 담당자는 구체적인 방안을 모색하여 안정성을 확보하여야 한다.
87. 제휴업체 및 업무위탁사의 접속: 외부 제휴업체 및 업무위탁사의 내부네트워크 접속에 대해 사용자별 인증절차를 마련하거나, 출발지 또는 목적지 주소별 통제, 프로토콜별 통제, 감사, 로그관리 등을 통해 통제하여야 한다.
88. 외부 전산시스템의 접속: 외부 전산시스템과의 연결은 전용선 연결을 원칙으로 한다.
89. 네트워크 담당자는 외부에서의 내부 네트워크 접속에 대해 보안사고 발생 여부를 점검하여야 한다.
90. 네트워크 접속통제 설정 후, 네트워크 담당자는 분기 1회 이상 네트워크 통제설정에 대한 유지 및 관리여부를 점검해야 한다.
91. 네트워크 담당자는 네트워크를 구성하는 자산들에 대한 “네트워크 자산 목록 및 구성도”를 작성하여야 한다.
92. 외부개발 용역 시 사용 네트워크를 내부 운영 네트워크와 분리함으로써 외부인력이 내부 네트워크에 불법적으로 접근하는 것을 제한하여야 한다.
93. 내부 조직 내 합법적인 승인 없이는 네트워크 패킷 모니터링을 못하도록 금지하여야 한다.
94. 무선 네트워크 관리
95. 무선랜의 범주에는 무선AP, 무선공유기, 무선브릿지, Ad-Hoc 네트워크 등을 모두 포함한다.
96. 회사의 중요한 정보시스템이 위치한 서버실, 취약점 분석실에는 무선AP의 설치를 금지한다. 단, 업무상 부득이하게 무선AP 설치가 필요한 경우에는 정보보호 최고책임자의 승인을 득한 후 보안조치를 적용한 후에 설치가 가능하다.
97. 회사 내에서 정보보호 최고책임자가 승인하지 않은 무선랜의 사용은 금지한다.
98. 네트워크 담당자는 회사 내에서 무선랜을 제공하려는 경우 패스워드 설정, MAC 주소 등록 등으로 통제하여야 한다.
99. 설치된 무선AP는 근무자가 접근이 용이하지 않은 장소(통제구역)에 설치 · 운영한다.
100. DB 보안
101. 도입 및 설치
102. DB는 정보보호 최고책임자가 정한 DB담당자에 한하여 관리할 수 있다.
103. DB운영부서는 관리하는 모든 DB 및 Table의 목록을 기록 • 관리하여야 한다.
104. DB담당자는 다음 각 호의 DB보안 운영업무를 수행한다.
105. 사용자계정관리 및 DB 접근권한관리 등 DBMS 운영업무
106. DB 접근권한 부여에 대한 적정성 검사
107. 로그파일에 대한 모니터링
108. 기타 DB보안 관리업무
109. 정보보호 최고책임자는 DB보안을 위하여 DB접근프로그램을 제한할 수 있다.
110. DB운영부서는 사용자 별로 접근권한을 통제하여야 하며, 데이터를 보호할 수 있는 자체 보안알고리즘을 갖추어진 DBMS를 사용하여야 한다.
111. DBMS는 다음 각 호의 보안기능을 갖추어야 한다.
112. 프로그램, 명령어 등의 데이터에 대한 접근통제 기능
113. DB 감시 기능
114. 특정 스키마객체나 특정한 운영만을 사용자에게 허가할 수 있는 기능
115. DB내의 장애나 데이터의 불일치를 검색하고 해결할 수 있는 기능
116. 로그의 기록 및 관리 기능
117. DB 암호화
118. DB데이터는 사용자가 직접 접근할 수 없으며, 어플리케이션을 통하여 데이터를 등록, 수정, 삭제하여야 한다. 단, 정보보호 최고책임자의 승인이 있는 경우 예외로 한다.
119. 데이터베이스 암호프로그램은 암 • 복호화를 병행하여 사용할 수 없다. 단, 장애 등 복호화가 필요한 경우 정보보호 최고책임자의 승인을 받아야 한다.
120. 응용 프로그램 보안
121. 관리자 접근 관리
122. 정보 및 응용프로그램 기능의 접근은 응용프로그램 접근통제 정책에 따라 제한하여야 한다.
123. 중요시스템은 전용 컴퓨터 환경에서 수행함으로써 다른 프로세스가 가용성이나 비밀성, 무결성에 영향을 미치는 일이 없도록 하여야 한다.
124. 개인정보를 처리하는 응용프로그램에서 불필요한 기능을 제공하여 권한을 우회할 수 없도록 조치하여야 하고, 우회방법이 존재할 경우 이를 방지하는 대책을 수립하여야 한다.
125. 중요 정보의 출력물에는 표지에 등급과 지정 배포처, 경고문 등이 표시되어야 하며 각 장마다 등급 및 문서번호를 표시하여야 한다.
126. 최대 15분 동안 입력이 없는 세션은 Time-out 설정을 통해 연결을 차단하여야 한다.
127. 중요한 응용 프로그램은 동일 사용자의 동시 세션 수를 제한하여 비인가된 접근을 검출할 수 있어야 한다.
128. 정보보호시스템 보안
129. 정보보호시스템 구성관리
130. 보안시스템은 IT보안 전담부서의 합의 없이 설치·운영 되어서는 안 된다
131. 보안시스템은 물리적 보안이 되어 있는 제한구역 및 통제구역에 설치한다.
132. 보안시스템을 설치한 후 보안시스템 담당자는 최신의 보안 이슈를 반영하여 패치 및 보안 설정을 적용한다.
133. 계약에 의해 보안시스템이 관리되는 경우 발생할 수 있는 데이터의 손상, 손실 등의 보안위험 및 대책을 계약서상에 반영하도록 한다.
134. 도입
135. 보안시스템 담당자는 운영 전 정보보호 최고책임자와 협의 후 보안시스템 도입을 진행하여야 한다.
136. 보안시스템 도입 시 보안시스템 담당자는 설계 변경, 증설 등의 환경 변화뿐만 아니라 도입불용의 요구가 있는지 모니터링 하여야 하며, 적절한 도입시기와 수요를 파악하여야 한다.
137. 시스템 운영
138. 보안시스템은 물리적으로 출입이 통제될 수 있는 시설에 설치되어야 하며, 불가피한 경우 시건 장치가 되어 있는 장소에 설치하여 일반인의 접근을 통제한다.
139. 통신망의 접근은 회선 유지보수업체 및 보안시스템 관리자를 제외한 인원의 접근을 통제하여야 한다.
140. 보안시스템에 대한 접근은 인터넷구간으로부터의 연결을 허용하여서는 안되며, 반드시 해당 장비에 직접 접속하는 것을 원칙으로 한다. 단, 외부 원격접속이 필요한 경우 별도의 보안 대책을 수립하여 정보보호 최고책임자의 합의 후 사용해야 한다.
141. 보안프로토콜을 지원하지 않는 경우 특정한 IP에서만 접근 가능하도록 접근제어를 설정해야 한다.
142. 개인정보처리시스템 보안
143. 개인정보 관리
144. 개인정보 관리책임자는 개인정보처리시스템 내의 개인정보보호를 위하여 다음의 기술적 보호조치를 수행하여야 한다.
145. 개인정보 보유, 취급 시스템은 침입차단시스템, 침입탐지시스템 등 정보보호시스템으로 보호
146. 백신프로그램의 설치•운영 등 컴퓨터바이러스 방지 조치
147. 암호알고리즘 등의 이용을 통하여 개인정보를 안전하게 네트워크상에서 전송할 수 있는 보안 조치
148. 개인정보 보유•취급 시스템 운영 부서는 주기적으로 취약점 진단을 수행하고 웜 바이러스에 대한 예방활동 시행.
149. 개인정보 관리책임자는 개인정보처리시스템이 외부시스템 또는 외부망과 연동 시 다음의 기술적 보호조치를 수행하여야 한다.
150. 개인정보 보유, 취급 시스템 연동 시에는 전용회선 등을 이용함으로써 정보 유출 위험 최소화
151. 시스템 연동 시 데이터의 복사 및 DB테이블 연동을 최소화하고 업무상 필요한 최소의 데이터만 송•수신
152. 개인정보를 회사 사내망이 아닌 외부망으로 송신할 때는 통신구간 암호화를 통하여 보호.
153. 개인정보 관리책임자는 개인정보처리시스템의 구축, 변경 등 아래의 각 호의 상황 발생 시 시스템 보안성 검토에 대하여 정보보호 최고책임자에 의뢰하여야 한다.
154. 개인정보를 보유, 관리해야 하는 정보시스템의 신규 구축 시
155. 신기술 또는 기존 기술의 통합으로 프라이버시 침해 가능성이 우려되는 기술을 사용하는 경우
156. 신규 사업 추진에 있어 프라이버시 침해 가능성이 제기될 가능성이 있는 경우
157. 개인정보를 보유, 관리하는 기존 정보시스템 변경 시
158. 개인정보의 사내 외 시스템간 연동 및 협력사 제공 시
159. 정보시스템 기획, 개발에 따른 보안성 검토 요청 시 개인정보보호와 관련된 사항 공동으로 검토 요청 가능

서비스 연속성 관리

1. 장애관리
2. 업무주관 부서는 정보시스템에 장애 발생 시 즉시 해당 해당 기술보안 담당자에게 이를 접수하여야 한다.
3. 해당 기술보안 담당자는 장애발생을 인지하는 즉시 효과적인 장애대응을 위해 업무주관 부서와 함께 비상대응체계를 구축한다.
4. 비상대응체계에 속한 모든 단위조직은 신속한 장애대응을 위해 적극적으로 협조하여야 한다.
5. 기술보안 담당자는 장애조치 후 장애영향도 및 조치내역에 대해 업무주관 부서에 통지해야 한다.
6. 기술보안 담당자는 장애조치 후 장애원인, 조치내역, 향후 개선방안 등 장애예방 및 사후관리에 필요한 정보를 포함한 장애보고서를 작성하여야 한다.
7. 가용성 관리
8. 업무연속성 관리체계를 수립하기 위해서는 프로젝트 팀이 구성되어야 되며 또한 체계를 유지관리하기 위해서는 적절한 조직구조를 구성하여야 한다.
9. 업무연속성관리를 위한 다음 단계와 같은 과정과 산출물 등이 포함된 방법론을 수립하여야 한다.
10. 개시단계
11. 업무연속성전략 수립단계
12. 구현단계
13. 운영관리단계 등
14. 개시단계에는 업무연속성관리에 대한 정책 수립 및 범위설정, 자원분배를 포함하여야 한다.
15. 업무연속성전략 수립단계에는 업무영향분석을 하여야 한다.
16. 구현은 기술적 대책, 조직 구성, 절차/지침의 문서화 등이 활동을 포함하여야 한다.
17. 운영관리단계에서는 시험, 교육ㆍ훈련, 검토 및 갱신 활동을 포함하여야 한다.
18. 조직의 업무연속성계획 수립을 위한 프레임워크를 수립하여야 한다.
19. 업무연속성 계획
20. 재난재해시나리오에 따라 업무영향분석을 수행해야 한다.
21. 영향 분석결과를 기초로 업무복구목표 및 복구를 위한 최소 요구사항을 적절하게 설정하여야 한다.
22. 업무복구목표와 요구사항에 적합한 업무연속성 전략을 수립하여야 한다.
23. 업무연속성전략을 이행하기 위한 실행계획 차원의 업무연속성계획을 수립하여야 한다.
24. 업무연속성을 위한 대책은 그 목적을 달성(효과성)할 수 있어야 하며 또한 최소의 비용으로 구현 및 유지관리(효율성)할 수 있어야 한다.
25. 업무연속성계획 이행을 위해 필요한 세부계획과 절차 등을 문서화하여야 한다.
26. 유지보수 관리
27. 시스템의 원활한 사용을 위하여 모든 시스템에 대하여 유지보수계약을 체결하여야 한다.
28. 유지보수 계약을 체결할 경우 “생활보안지침, 제\*\*조(외부 위탁 계약시 보안 통제)”를 준용하며 다음 사항을 포함하여야 한다.
29. 시스템의 원활한 사용을 위한 유지보수업체의 예방점검
30. 장애(Parts 교체) 시 유지보수업체의 즉각적인 지원
31. 기타 원활한 시스템 운영을 위해 정보보호 담당자가 판단한 필요 사항

외주인력 보안

1. 보안 통제
2. 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.
3. 제3자에 의하여 제공되는 서비스는 주기적인 감시, 감독이 되어야 하며, 기록 · 관리되어야 한다.
4. 제3자 서비스의 변경 시 관리조직은 위험의 재평가와 관련된 사업 시스템 및 프로세스의 중요도를 고려하여 기존의 정보보호 정책의 유지/개선을 포함한 서비스 공급에 대한 변경을 관리하여야 한다.

출입통제 관리

1. 일반 관리
2. 원칙
3. 정보보호 최고책임자는 회사의 주요 정보자산 및 관련 시설에 대한 보안강화를 위하여 다음 각 호와 같은 보호구역을 지정 및 운영하여야 한다.
4. 제한구역: 회사의 중요정보가 사용되어 임직원은 출입 가능하나, 외래인 및 방문자에 대한 출입 안내가 요구되는 구역
5. 통제구역: 회사의 핵심적인 정보가 사용 및 보관되어 임직원 또한 출입 허가를 득한 자만 출입이 가능한 구역
6. 지정된 보안구역은 “보안구역 현황”에 따른다.
7. 정보보호 최고책임자는 제한구역의 출입통제를 위하여 카드 잠금장치, 지문인식 잠금장치 등 출입통제 장치를 설치 및 운영하여야 한다.
8. 제한구역을 출입하는 모든 출입자는 반드시 출입증을 패용하여야 한다.
9. 외부인력의 제한구역 출입은 업무상 필요에 따라 결정되어야 하며, 수행직원은 외부인력과 동행하여 제한구역에서의 활동을 지속적으로 감독하여야 한다.

1. 출입권한 관리
2. 정보보호 관리자는 임직원, 파견직, 계약직, 외주용역 직원 등 회사에서 근무하는 모든 근무자(이하 “근무자”라 한다)에 대한 출입을 통제하여야 한다.
3. 임직원에 대하여는 입사 시 인사발령에 의하여 물리보안 담당자가 출입카드를 발급한다.
4. 업무상 고정 출입을 해야 하는 외부업체 직원의 경우 담당부서장은 정보보호 관리자의 승인을 득하고, 물리보안담당자에게 출입증 발급을 의뢰하여야 한다.
5. 임시 방문자에게 출입증을 발급하여야 하는 경우에는 방문자의 신원을 확인할 수 있는 서류(주민등록증, 운전면허증, 주민등록등본 등이나 그 사본)를 제출하거나, 방문의 목적이 되는 담당자의 확인을 거쳐 출입증을 발급하여야 한다. 단, 단체 방문자의 경우 대표자에게만 출입증을 발급한다.
6. 다음 각 호의 방문자는 출입증 교부 대상에서 제외할 수 있다.
7. 회사 업무와 관련하여 신원이 확인된 국내의 저명인사
8. 단체 방문자 중 대표자를 제외한 인원
9. 물리보안 담당자는 근무자 또는 방문자에 대한 출입증 교부사실을 “출입증 관리대장”에 기록하고 관리하여야 한다.

1. 통제구역의 관리
2. 통제 구역 설정
3. 통제구역은 불특정 다수인이 출입하는 장소로부터 격리하여 제3자가 침입할 우려가 적은 장소에 설치하여야 한다.
4. 물리보안 담당자는 통제구역에 대한 보안통제에 관한 사항을 별도의 지침서로 작성 및 운영할 수 있다.
5. 통제구역의 출입문에는 출입자가 통제구역임을 쉽게 인지할 수 있도록 별도의 표시를 하여야 한다. 단, 통제구역 표시의 크기 및 재질 등은 시중에서 판매하는 제품을 구매하여 사용할 수 있다.
6. 통제구역은 출입통제를 위하여 별도의 출입통제장치를 설치하여야 한다.
7. 통제구역의 출입문은 자동으로 잠김이 가능하여야 한다.
8. 비인가자가 통제구역 출입이 필요한 경우에는 해당 부서의 장이 출입할 인원에 대한 소속, 성명, 사유, 보안대책 등을 명시하여 정보보호 관리자에게 요청 후 승인을 얻어야 한다.
9. 정보보호 관리자는 통제구역 출입 허가 이력을 “통제구역 출입관리대장”에 기록 및 유지하여야 한다.
10. 물리보안 담당자는 통제구역 출입자의 출입로그를 3개월 이상 보관하여야 한다.
11. 모든 임직원은 비인가자의 불법접근 또는 시도를 인지한 경우, 정보보호최고책임자 및 정보보호 관리자에게 즉시 보고하여야 한다.
12. 통제구역 내에 사진, 비디오 등 촬영장비 및 녹음기 등의 기타 저장장치의 반입은 금지한다. 단, 업무상 필요에 따라 정보보호 관리자의 승인을 받은 경우는 예외로 한다.
13. 정보보호 관리자는 통제구역의 출입로그를 분기 1회 점검하여야 한다.
14. 출입 통제
15. 정보보호 최고책임자는 근무자 및 방문자의 출입을 일부 지역에 한하여 통제할 수 있으며, 방문자의 출입을 요청한 부서에 인솔 및 안내를 요구할 수 있다.
16. 방문자의 출입을 요청한 부서는 방문자가 회사에 들어와서 나갈 때까지 정보자산의 불법 반출이 발생하지 않도록 관리할 책임이 있으며, 이상 징후 발견 시 정보보호최고책임자 및 정보보호 관리자에게 즉시 보고하여야 한다.
17. 방문자의 출입을 요청하는 경우에는 정보보호 관리자에게 방문자의 인적사항, 사유, 장소 등을 사전에 요청해야 한다. 이때 정보보호 관리자는 “방문자 기록대장”의 양식에 따라 그 이력을 유지하여야 한다.
18. 휴일에 회사에 출입하여 근무하여야 하는 경우 근무자는 해당 부서의 팀장에게 그 사실을 사전 통보하여야 하며, 각 부서의 팀장은 그 사실을 정보보호 관리자에게 알려야 한다. 단, 메일을 통하여 근무자가 해당 부서의 장에게 휴일 근무를 알리는 경우 정보보호 관리자를 ‘참조자’에 넣어야 하며, 이 경우 해당 부서의 팀장은 정보보호 관리자에게 별도의 통보 의무가 없다.
19. 외부인은 휴일에 회사에 출입할 수 없다. 단, 다음 각 호의 경우는 별도의 승인을 얻어 예외로 할 수 있다.
20. 시설보수, 장애 등의 긴급 업무처리를 위하여 담당 직원이 동행한 경우
21. 외부업체 직원 중 휴일 업무에 대해 소속 부서 팀장의 사전 승인을 득한 경우
22. 업무처리를 위해 해당부서 임직원이 동행한 경우
23. 기타 정보보호최고책임자의 승인을 득한 경우
24. 통제구역 내 작업
25. 서버, 네트워크 장비, 정보보호시스템, 백업장치 등 정보시스템 특성에 따라 분리하여 배치하고, 전산랙(Rack)등을 이용하여 시스템을 보호하여야 한다.
26. 전산랙(Rack)은 잠금장치를 설치하는 등 인가된 자에 한해 접근이 가능하도록 관리하여야 한다.
27. 기술보안 담당자는 전산장비의 분해, 부품교환 등의 유지보수 시 사전에 정의된 절차에 따라 수행하는지 확인해야 하며 전산장비 별 유지보수 내역과 의심되는 결함을 “전산장비 유지보수 기록 대장”에 기록 및 관리하여야 한다.
28. 전산장비는 환경상의 위협을 최소화 할 수 있도록 배치하고 비인가자의 침해를 방지할 수 있도록 보호하여야 한다. 특히 전산장비 주위에서의 흡연 및 취식은 금지한다.
29. 업무용 PC를 제외한 모든 전산장비는 통제구역에 배치하여야 한다. 특히 정보자산이 집중되는 파일서버, DB 등은 통제구역 내 별도의 공간에 잠금장치의 설치가 가능한 전용 캐비닛에 설치하여야 한다. 단, 장비의 구성에 따라 정보보호최고책임자가 그 설치를 유보할 수 있다.
30. 서버실은 케이블이 안전하게 유지되도록 전용 통로관 설치 등의 적절한 보호조치를 강구해야 한다.
31. 배달 및 하역 구역의 분리
32. 서버실 및 연구소에서의 비정상적인 작업을 통제하고 인프라의 불법적인 반입·반출을 예방하기 위해 배달 구역과 작업 장소를 명확히 분리하여야 한다.
33. 서버 및 네트워크 담당자는 배달 구역과 작업 장소에서 하여 및 배달되는 인프라를 확인하여야 한다.
34. IT 인프라 보호
35. 보호대책
36. 물리보안 담당자는 지진, 수해 및 화재 등으로 인한 서버실의 전력공급 중단에 대비하기 위하여 다음 각 호에 해당하는 보안대책을 강구해야 한다
37. 전력공급의 일시 중단에 대비하여 UPS와 축전지 설비의 보유
38. 배전반에 단락, 지락, 과전류 및 누전을 방지할 수 있도록 인프라 설치
39. 주요시설에 대한 비상조명 설치
40. 물리보안 담당자는 각종 전원인프라를 보호하기 위하여 다음 각호에 해당하는 보안대책을 강구해야 한다.
41. 주요시설의 각종 전원인프라에 대한 접지시설 설치
42. 물리보안 담당자는 시설의 안전점검을 실시하여 점검 결과 나타난 문제점을 조치하여야 한다.
43. 기타 건물 자체적인 설비 관련 사항은 물리적 보안 담당자와 사옥 및 IDC 자체 관리 부서의 협의를 통해 추가적인 대비책을 강구한다.
44. 케이블 보호
45. 배전반, 전화 단자함 등은 잠금장치를 설치하는 등 인가된 자에 한해 접근이 가능하도록 관리하여야 한다.
46. 전산장비에 연결된 전력과 통신 케이블은 절단 등의 위협으로부터 보호하기 위해 가능한 매설하고, 매설이 어려울 경우 보호용 파이프 등을 사용하여 보호해야 한다.
47. 일반구역이나 케이블이 외부에 노출 될 위험이 예상되는 지역은 우회하여 케이블을 설치한다.
48. 인프라 반출
49. 모든 근무자는 다음 각 호의 물품에 대하여 반출‧입을 하여서는 안 된다. 단, 소속 팀장 및 정보보호 관리자의 승인을 받은 경우는 예외로 한다.
50. 개인소유의 PC 및 휴대용 전산장비(노트북, 태블릿 PC 등)
51. 회사의 중요정보 및 개인정보가 포함된 문서 또는 저장매체
52. 기타 정보보호최고책임자가 통제대상 물품으로 추가 지정한 물품
53. 반출‧입 통제대상 물품은 업무시간 중에 반출입하여야 한다. 단, 사전에 정보보호 관리자의 승인을 받은 경우에는 예외로 한다.
54. 장비 유지보수를 위한 반출‧입 시에도 중요정보 및 개인정보를 삭제하거나 암호화하여 이를 통한 정보유출이 발생하지 않도록 하여야 한다.
55. 반출‧입 통제대상 물품을 반입하고자 하는 경우에는 정보보호 관리자의 승인을 받아야 한다. 이때 해당 임직원 및 해당 부서의 장은 통제대상 물품의 보안관리 책임을 가지며, “물품 반출입대장”을 작성 후 정보보호 관리자에게 통보하여야 한다.
56. 정보보호 관리자는 반입하려는 물품에 대하여 다음 각 호의 내용을 확인하여야 하며, 안전성 여부의 판단이 불가능할 경우 반입 요청자의 확인 전까지 반입을 제한할 수 있다. 단, 귀중품, 포장물품 등 그 내용을 확인할 수 없는 물품인 경우에는 지정된 장소에서 반입 요청자에 의해 확인한다.
57. 해당 물품의 반입요청자, 출입자, 출입시간, 사전 요청여부 (단, 반입물품의 품목‧상태‧수량은 물품 반입 요청자가 확인한다.)
58. 총포, 화약 등 안전 위해 물품 여부
59. 전자기 발생, 과도한 자기장 형성 등 시스템 운영 및 정보자산 관리에 대한 영향 발생 여부
60. 기타 회사 보안관리에 위해 하다고 판단되는 물품여부
61. 반출‧입 통제대상 물품을 반출하고자 하는 경우에는 정보보호 관리자의 승인을 받아야 한다. 단, 긴급한 상황인 경우 구두로 선 처리하고 사후 승인을 받아야 하며 해당 부서의 장은 “물품 반출입대장”을 기록하여 정보보호 관리자에게 통보하여야 한다.
62. 전산장비를 반출하고자 하는 경우 해당 부서장은 회사가 정한 방법에 따라 포맷 등의 방법을 통해 저장매체에 기록되어 있는 데이터를 복구할 수 없도록 삭제한 후 반출을 승인하여야 한다. 단, 전산장비의 포맷이 불가능한 경우 해당 부서장은 회사의 주요 정보자산 존재 유무를 확인하고 반출 확인을 하여야 한다.
63. 반출 통제대상 물품에 포함된 각종 정보삭제 여부, 반출의 필요성, 소유권의 확인, 수량 등에 대한 검토 및 확인 책임은 반출 해당 부서장이 가진다.
64. 정보보호 관리자는 프로젝트의 투입 등 장기간 혹은 잦은 반출로 승인이 원활하지 못할 것으로 판단되는 경우 분기별로 일괄 승인할 수 있다.

끝.

**부 칙**

**(시행일)** 이 정책은 2018. 10. 05 부터 시행한다.