DOC-POL-004

**개발보안 지침**

개정번호 : 1.00

**㈜1 Shop**

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

**목 차**

[제1장 개 요 5](#_Toc381351704)

[제1조 목적 5](#_Toc381351705)

[제2조 적용대상 5](#_Toc381351706)

[제2장 개발 단계 별 보안 5](#_Toc381351707)

[제1절 기획 단계 5](#_Toc381351708)

[제3조 요구사항 정의 5](#_Toc381351709)

[제2절 설계 단계 6](#_Toc381351710)

[제4조 요구사항의 반영 6](#_Toc381351711)

[제5조 사용자 계정 설계 7](#_Toc381351712)

[제6조 비밀번호 설계 7](#_Toc381351713)

[제7조 인증관리 7](#_Toc381351714)

[제8조 접근권한 설계 8](#_Toc381351715)

[제9조 로그인 설계 9](#_Toc381351716)

[제10조 암호화 설계 9](#_Toc381351717)

[제11조 로그관리 설계 10](#_Toc381351718)

[제3절 구현 단계 11](#_Toc381351719)

[제12조 안전한 코딩 11](#_Toc381351720)

[제13조 취약성 점검 12](#_Toc381351721)

[제4절 테스트 단계 12](#_Toc381351722)

[제14조 응용 프로그램의 테스트 12](#_Toc381351723)

[제15조 테스트 데이터의 사용 13](#_Toc381351724)

[제16조 보안성 검토 14](#_Toc381351725)

[제5절 이관 및 배포단계 15](#_Toc381351726)

[제17조 이관 절차 15](#_Toc381351727)

[제18조 운영 환경 16](#_Toc381351728)

[제6절 개발환경 보안 16](#_Toc381351729)

[제19조 개발, 운영 환경의 분리 16](#_Toc381351730)

[제20조 소스 코드 관리 17](#_Toc381351731)

[제21조 변경 관리 17](#_Toc381351732)

[제22조 계정 관리 18](#_Toc381351733)

[제23조 개발용 DB 보안 관리 18](#_Toc381351734)

[제24조 폐기 및 기타 19](#_Toc381351735)

[제25조 외주 개발 보안 관리 19](#_Toc381351736)

개 요

1. 목적

본 지침은 (주)1 Shop(이하 ‘회사’라고 한다)의 어플리케이션의 개발 시 검토되어야 할 정보보호 통제를 소프트웨어 수명주기 별로 작성하여 어플리케이션의 보안성, 안전성, 신뢰성을 확보함을 목적으로 한다.

1. 적용대상

본 지침은 서비스 및 업무용 어플리케이션 등 회사에서 내부직원 및 외부 위탁을 통해 개발되는 모든 어플리케이션을 그 적용 범위 및 대상으로 한다.

개발 단계 별 보안

1. 기획 단계
2. 요구사항 정의
3. 사업부서 담당자는 서비스 기획 단계에서의 정보보호 요건을 정의하고 사업부서 관리자의 승인을 거쳐 개발 담당자에게 개발을 요청한다.
4. 사업부서 담당자는 서비스 기획 시 개인정보를 취급하는 경우 사업부서 관리자의 승인을 거쳐 개인정보 관리자에게 개인정보영향평가를 의뢰하여야 한다.
5. 개발 담당자는 서비스 기획에 따른 응용프로그램 개발 요청 내용을 검토하여 다음의 정보보호 요건 등을 정의하고 필요 시 사업부서 담당자와 협의하여야 한다.
6. 사용자 식별 및 인증
7. 권한관리 및 접근통제
8. 암호화 등 주요정보의 기밀성과 무결성을 확보할 수 있는 방안
9. 로깅기록 및 감사
10. 장애 발생 시 가용성 확보
11. 클라이언트 통제
12. 개인정보보호 관련 사항
13. 개발 담당자는 응용프로그램에서 요구되는 보안 요구사항과 최신 보안 이슈에 대하여 정보보호 담당자에게 문의할 수 있다
14. 설계 단계
15. 요구사항의 반영
16. 정보보호 관리자는 요건정의 및 분석 시 다음의 정보보안 사항들을 고려하여 응용프로그램 개발에 반영하도록 조치한다.
17. 기존 시스템과의 연동성
18. 기존 시스템의 정보 보안에 대한 위협 가능성
19. 관련 법규 준거성
20. 정보보호, 개인정보보호 유관 법률
21. 회사 규정 내 요구사항
22. 취급하는 고객/직원 정보, 영업비밀 등 중요 개인정보보호를 위한 보안요구사항
23. 개발 담당자는 응용프로그램에서 요구되는 보안 요구사항과 최신 보안 이슈에 대하여 정보보호 관리자 및 담당자에게 문의할 수 있다.
24. 사용자 계정 설계
25. 사용자 계정 체계는 사용자 별로 유일한 고유계정을 부여할 수 있도록 설계하여야 하며, 이미 부여한 계정을 타인에 의해 재사용이 불가하도록 설계하여야 한다.
26. 비밀번호 설계
27. 개발 담당자는 비밀번호의 최소 길이 통제 및 비밀번호를 사용할 수 있는 최소/최대기간을 설정할 수 있도록 있도록 설계하여야 한다.
28. 비밀번호의 길이는 최소 8자 이상이어야 하며 영문자, 숫자 및 특수문자를 포함하여야 한다. 비밀번호 조합원칙은 다음과 같다.
29. 3가지 조합(영어 대소문자/특수문자/숫자)일 경우 8자 이상
30. 2가지 조합(영어 대소문자/숫자)일 경우 10자 이상
31. 비밀번호 변경: 최소 6개월(반기)에 1번 변경/ 권고는 3개월임
32. 개발하는 모든 어플리케이션의 비밀번호는 주기적으로 바꿀 수 있도록 개발하여야 한다. 이 때 이전에 사용한 패스워드는 180 일 이상 사용할 수 없으며 이전과 동일한 비밀번호를 사용할 수 없도록 하여야 한다.
33. 사용자가 비밀번호를 분실한 경우 비밀번호를 초기화할 수 있도록 설계하여야 한다.
34. 개발 담당자는 모든 어플리케이션이 사용자가 비밀번호를 입력하는 화면상에서 읽을 수 없는 형태로 표시(masking)되도록 설계하여야 한다.
35. 개발 담당자는 어플리케이션 접근비밀번호를 DB에 저장할 때 암호화하여 저장하여야 하며, 사용자 인증 시 암호화한 상태에서 검증하여야 한다.
36. 인증관리
37. 개발되는 어플리케이션은 사용자의 권한을 확인한 후 작동되도록 설계해야 한다.
38. 어플리케이션에 대한 인증 수단은 개발 담당자, 개발을 의뢰한 현업 부서, 정보보호 관리자 등 관련 부서의 협의 하에 최적의 인증 수단을 선택하고 정보보호 최고책임자가 결정한다.
39. 특별한 관리가 요구되는 비밀 정보는, 인가된 내부자의 실수에 의한 중요정보 유출 혹은 삭제의 위험을 방지하기 위해 추가적인 인증 절차가 이루어질 수 있도록 한다.
40. 인증 정보는 일방향 암호화된 상태로 관리되어야 한다.
41. 비밀번호의 일방향 암호화 암호화를 위한 해쉬함수로 SHA 256을 사용 한다.
42. 사용자 인증 데이터의 저장과 전송 시 암호화에 대한 세부 내용은 “제10조 암호화 설계”에 따른다.
43. 접근권한 설계
44. 개발되는 어플리케이션은 사용자 접근 시 인증과정을 거치도록 설계하여야 하며, 사용자 계정 별로 접근권한을 통제할 수 있도록 설계하여야 한다.
45. 어플리케이션의 설계 및 개발 시 업무 성격상 또는 업무 흐름상으로 적절하도록 화면 및 메뉴 별로 접근 권한을 통제한다.
46. 어플리케이션의 사용자를 사용자, 직책, 부서별 인가된 등급 등으로 구분하여 접근 권한을 관리할 수 있도록 한다.
47. 필요한 경우 날짜, 시간, IP Address별로 사용자의 접근을 통제할 수 있도록 한다.
48. 하나의 사용자 및 관리자 계정으로 여러 터미널, IP address, 다중 session에서 동시에 둘 이상의 온라인 세션을 연결하지 못하도록 한다.
49. 사용자로부터 최대 15분 동안 어떤 입력도 일어나지 않는 경우 자동적으로 로그오프(logoff)시키거나 세션이 종료되도록 구현한다.
50. 사용자가 특정시간 동안 해당 어플리케이션을 사용하지 않을 경우, 업무 내용 보호를 위하여 세션 잠금 등 보호 대책을 구현한다.
51. 로그인 설계
52. 로그인 화면에서는 단지 로그인 관련 정보만 표시될 수 있도록 한다. 운영체제, 네트워크 환경, 내부적인 사항과 같은 정보는 로그인 과정을 성공적으로 마친 후 표시될 수 있도록 한다.
53. 특별한 경우를 제외하고는 사용자가 로그인하기 전에 보안 경고 문구를 표시하여 사용자들의 보안에 대한 경각심을 고취할 수 있도록 한다.
54. 어플리케이션 사용자의 로그인 실패 시 로그인 실패 이유를 표시하지 말고, 단순히 로그인 절차가 잘못되었다는 정보만 표시하고 세션을 종료 시키거나 정확한 로그인 정보가 입력되기를 기다리도록 한다. 단, 로그인 실패 이유를 상세하게 표시할 필요성이 인정되는 경우는 예외로 할 수 있다.
55. 어플리케이션 사용자가 5회 이상 비밀번호를 잘못 입력할 경우 일시적으로 사용을 중지시키거나 세션을 종료시키도록 한다. 충분한 본인 확인 과정을 거친 후 임시 비밀번호를 부여하여 로그인 후 비밀번호 변경을 안내하도록 설계한다.
56. 어플리케이션 사용자가 로그인 하였을 경우, 해당 사용자가 자신의 로그인 정보를 확인하고, 비인가자에 의한 해당 계정으로의 로그인 여부를 확인할 수 있도록 하기 위해 가장 최근에 성공적으로 로그인한 날짜, 시각 등의 정보를 화면에 표시할 수 있도록 한다.
57. 동시에 동일 ID로 접속하는 것을 허용하지 않도록 구현되어야 하며, 이런 경우 사용자에게는 로그인을 시도하는 사용자가 있다는 경고 메시지를, 로그인 하고자 하는 사용자에게는 이미 로그인한 사용자가 있다는 경고 메시지를 표시한다.
58. 암호화 설계
59. 법률에서 정하는 중요 개인 정보(주민번호, 비밀번호, 금융정보 등)를 전송할 때에는 암호화하여야 한다.
60. 법률에서 정하는 중요 개인 정보(주민번호, 비밀번호, 금융정보 등)는 암호화하여 DB에 저장하여야 한다.
61. 회사에서 사용하는 암호 정책은 관련 법률에서의 요구사항을 기준으로 국가에서 권장하는 암호 표준을 사용해야 한다.
62. 관련 법률에서 요구하는 구체적인 암호화 대상 및 암호화 방법은 문서화하여 관리한다.
63. 일방향 암호화를 위한 해쉬함수: 비밀번호 저장시, SHA 256 이상
64. 양방향 암호화: 주민번호, 신용카드번호, 은행계좌번호, 여권번호 등, AES 256이상
65. 원칙적으로는 주민번호의 경우 전체 13자리 모두 암호화해야 하나, 부하 발생시 뒷 7자리만 암호화할 수 있음
66. 신용카드도 원칙적으로는 모두 14자리. 13자리 암호화해야 하나, 부하 발생시 카드유형을 제외한 뒷 10자리를 암호화할 수 있음
67. SSL 인증서: 베리사인 128비트 이상(FIPS 140-2 호환) / RSA 는 2048 이상임
68. 보안채널은 모두 Https:// 사용함 (443포트 오픈), 제큐어 웹 등 보안프로그램은 사용자제 권고
69. 로그관리 설계
70. 설계 단계에서 고려된 응용프로그램 로그 관리 기능에 따라 로그를 기록하고 최소 3개월 이상 보관한다. 단, 법적으로 요구하는 민감한 정보(금융정보 등)는 관련 법규를 따른다.
71. 중요한 정보를 취급하는 어플리케이션은 중요 정보의 입력, 수정, 삭제와 관련한 사용자의 활동 및 권한변경에 관련된 로그를 기록하도록 설계한다.
72. 어플리케이션은 보안감사를 위하여, 생성된 로그를 분석하여 보고서를 작성할 수 있도록 다음과 같은 보안감사 로그 기능을 가지도록 설계한다.
73. 보안감사 로그 데이터는 주체, 객체, 사건, 시간정보 및 사건의 결과 등을 반드시 포함해야 한다.
74. 관리자 및 사용자의 로그인로그아웃, 사용자 인증정보 및 권한의 변경, 어플리케이션의 시작중지, 특수권한의 수행(시도) 및 기타 중요한 어플리케이션 사건 등을 포함해야 한다.
75. 접근통제 요구사항을 비롯한 보안감사 로그의 비밀성 및 무결성 보장 방안을 추가해야 한다.
76. 구현 단계
77. 안전한 코딩
78. 개발자는 응용프로그램 개발에 적합한 언어를 선택할 때 개발언어의 보안성을 고려하고, 각 개발언어의 보안상 알려진 취약점에 대해 정보보호 담당자에게 문의하여 숙지해야 한다.
79. 응용프로그램에 대한 정보보호 요구사항은 응용프로그램 설계 단계에서부터 테스트 후 운용될 때까지 응용프로그램 개발자에 의해 일관성 있게 적용될 수 있도록 한다.
80. 응용프로그램 및 라이브러리의 정보보호 침해를 예방하기 위해 개발 중인 응용프로그램 및 라이브러리는 운영시스템에 저장되지 않도록 한다.
81. 정보보호 관리자는 외부인에 의해 응용프로그램 개발 시 위험 요소를 파악하고 통제 하여야 한다.
82. 응용프로그램 개발 시 최신 시큐어코딩 가이드라인을 준수하여야 한다.
83. 취약성 점검
84. 개발부서는 어플리케이션 설계 • 개발 시 중대한 보안위험이 판단되는 경우 정보보호 최고책임자에게 취약성 점검을 요청하여야 한다.
85. 정보보호 최고책임자는 어플리케이션에 보안대책이 필요하다고 판단되는 경우 개발조직에 해당사항의 수정을 요청할 수 있다.
86. 개발 담당자는 취약성 점검 결과에 따라 응용프로그램에 존재하는 보안 취약점을 제거한다.
87. 정보보호 최고책임자는 필요 시 추가 취약점점검을 실시할 수 있고, 개발 담당자는 적극적으로 협조하여야 한다.
88. 테스트 단계
89. 응용 프로그램의 테스트
90. 개발 담당자는 새로운 어플리케이션 개발 후 테스트 시스템에서 해당 어플리케이션을 충분히 테스트하고, “어플리케이션 테스트 케이스”를 작성하여 정보보호 최고책임자의 승인을 득한다.
91. 어플리케이션의 개발에 요구사항이 반영되었는지의 여부를 확인하기 위한 테스트의 종류와 방법은 다음과 같다.
92. 단위 테스트: 어플리케이션의 최소 구성요소가 되는 모듈들에 대해 개별적으로 테스트를 시행하여 어플리케이션 개발 요청서에 기술된 기능이 제대로 수행되는지를 테스트 한다.
93. 통합 테스트: 단위 테스트를 통과한 모듈을 모아서 전체 어플리케이션을 완성하기 위해 통합적으로 시행하는 테스트로, 최소의 모듈을 연결하여 작은 구성요소로 통합 테스트를 하고, 점진적으로 다른 구성요소를 연결하면서 전체 어플리케이션을 테스트 한다.
94. 인수 테스트: 어플리케이션을 완성된 제품으로 보고 실제 자료를 사용하여 응용프로그램을 테스트하는 과정으로, 어플리케이션이 실질적으로 사용되기 위해 마지막으로 시행하는 테스트이다.
95. 입력/출력데이터의 유효성 점검 기능에 대하여 테스트 수행 시 다음과 같은 내용이 포함되어야 한다.
96. 한계 값을 넘는 값의 입력
97. 데이터 영역에 잘못된 문자의 입력
98. 불완전한 데이터의 입력
99. 데이터의 크기가 메모리 할당 범위를 벗어난 입력
100. 출력 데이터의 타당성
101. 출력 데이터의 정확성
102. 테스트 데이터의 사용
103. 어플리케이션을 테스트할 때는 운영 데이터의 노출을 방지하기 위해 임의의 테스트 데이터를 생성하여 활용하거나 운영 데이터를 변경하여 사용하도록 한다.
104. 운영 데이터를 테스트 데이터로 사용할 때에는 개발 담당자가 정보보호 관리자의 승인을 득한 후 주요 데이터필드(사용자 비밀번호, 주민번호 등)를 임의의 데이터로 변경하여 사용한다.
105. 특수한 테스트 사유로 인해 임의 데이터 생성 및 운영 데이터 변경이 어려운 경우 테스트 장비에 대한 IP기반의 접근통제를 구현하여 통제하도록 하고 테스트 완료 후 해당 데이터를 삭제하도록 한다.
106. 정보보호 관리자는 테스트용 데이터가 승인된 범위에 따라 적절하게 운영되고, 사용 이후에 삭제되었는지를 다음과 같이 점검한다.
107. 점검 대상

정보보호 관리자는 개발/테스트 PC 및 개발자 업무용 PC를 대상으로 점검한다.

1. 점검 주기

정보보호 관리자는 분기 점검 혹은 필요한 경우 상시 점검으로 테스트 데이터의 사용 적절성 여부와 사용 이후의 삭제 여부에 대해 실제 확인하며, 그 결과를 정보보호 최고책임자에게 보고한다. 외주에서 제3자가 개발업무를 수행할 경우, 분기 점검은 제3자 보안점검 수행 시 테스트용 데이터 보안관리 준수에 대한 점검항목을 포함하여 수행한다. 또한 상시 점검은 정보보호최고책임자의 승인을 받아 해당 업체에 미리 통보하여 점검을 수행하도록 한다.

1. 감독/검사 조치 및 보고

정보보호 관리자는 개발 담당자가 검사결과에 대한 조치를 실행하도록 요구하고 그 결과를 확인한다.

1. 개발부서는 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 정보보호 관리자의 승인을 받아 사용하고, 사용완료 즉시 실 데이터를 삭제하여야 한다.
2. 보안성 검토
3. 개발 담당자는 어플리케이션을 운영 단계로 이관하기 전에 정보보호관리자로부터 해당 어플리케이션에 대한 사전 보안성 검증을 받도록 한다.
4. 보안성 검증 대상은 신규 프로젝트에서 개발되어 운영단계로 이관하기 전 상태에 있는 어플리케이션으로 한다. 보안성 검증을 이미 받았으나 운영 단계에서 수시로 변경이 일어날 수 있는 어플리케이션은 해당 개발 담당자와 정보보호 관리자의 협의 하에 보안성 검증 대상을 결정하도록 한다.
5. 사전 보안성 검증 절차
6. 어플리케이션에 대한 사전 보안성 검증은 정보보호관리자가 사전 보안성 검증항목에 따라 실시하는 것을 원칙으로 한다. 단, 어플리케이션의 양이 방대하거나 기타의 필요성이 인정되는 경우 정보보호 최고책임자의 승인을 얻어 개발에 참여한 개발자도 사전 보안성 검증을 실시할 수 있다.
7. 사전 보안성 검증이 완료되면 정보보호관리자는 “보안성 검토 조치 결과서”를 작성하여 해당 어플리케이션 기능의 적절성 여부를 판단한다.
8. 사전 보안성 검증은 정보보호 최고책임자가 이에 대한 승인을 함으로써 효력을 발휘하게 된다.
9. 사전 보안성 검증 결과는 모두 문서화하여 관리하도록 한다.
10. 이관 및 배포단계
11. 이관 절차
12. 응용프로그램을 운영 단계로 이관하기 전 개발 담당자는 관리를 위한 최소한의 접근 권한을 제외한 모든 접근권한을 제거한 후 운영단계로 이관될 수 있도록 하여야 한다.
13. 정보보호 관리자는 응용프로그램을 적용한 후, 기존의 운영 환경에 미치는 영향을 분석하고, 이상이 발생할 경우 시스템 운영부서와 협업하여 문제를 해결해야 한다.
14. 정보보호 최고책임자는 개발 테스트 및 보안검수가 완료된 어플리케이션을 테스트 시스템에서 운영시스템으로 이관 • 운영하여야 하며, 운영시스템 이관은 개발자가 아닌 직무가 분리된 정보보호최고책임자가 별도 지정한 이관 담당자에 의해 수행하여야 한다.
15. 이관담당자, 개발자, 시스템 운영자를 분리하여 각각의 역할을 지정하여야 한다.
16. 조직규모 또는 업무분장으로 인해 개발 인력과 운영 인력의 분리가 불가한 경우에는 정보보호 최고책임자가 이관 작업 시 동석하여 개발 인력이 운영 시스템에 이관하는 과정에서 발생 가능한 보안상의 문제에 대해 감독 하여야 한다.
17. 정보보호 최고책임자는 테스트 시스템에서 운영 시스템으로의 이관프로세스를 수립하고, 동 프로세스에 따라 어플리케이션이 이관될 수 통제하여야 한다.
18. 이관 담당자는 프로그램소스와 실행모듈간의 버전을 확인하고, 일치된 실행모듈을 운영시스템에 적용하여야 한다.
19. 운영 환경
20. 개발 담당자는 개발 중이거나 중요한 변경이 발생한 어플리케이션에 대해 운영 단계로 이관하기 전에 사용자 매뉴얼을 작성하도록 한다. 사용자 매뉴얼에는 해당 어플리케이션에 대한 사항 및 어플리케이션에 적용된 보안에 관련된 사항도 함께 기술되도록 한다.
21. 어플리케이션을 운영 단계로 이관하기 전 개발 담당자는 공식화된 접근 권한을 제외한 모든 접근 권한을 제거한 후 운영단계로 이관하도록 한다.
22. 중요 어플리케이션은 최초 프로그램 실행 전에 복사본을 별도로 보관해 두어 만약의 사태에 대비하도록 한다.
23. 개발환경 보안
24. 개발, 운영 환경의 분리
25. 응용프로그램 운영 환경은 회사의 직원 네트워크 등과는 분리되도록 고립된 환경으로 구성되어야 한다.
26. 개발 시스템(테스트 포함)과 운영시스템은 물리적으로 분리되어야 한다.
27. 컴파일러, 편집기 등과 같이 개발에 필요한 도구는 운영 환경에 설치되지 않도록 한다.
28. 개발부서는 운영시스템에서 어플리케이션을 개발 또는 변경할 수 없다.
29. 운영시스템에는 개발 중인 소스코드나 목적코드를 저장할 수 없다.
30. 소스 코드 관리
31. 개발부서는 어플리케이션 개발 시 소스코드에 대한 변경이력을 관리하는 절차를 수립하여야 한다.
32. 개발 중인 프로그램 및 데이터 라이브러리는 운영시스템에 저장할 수 없다.
33. 프로그램 소스에는 시스템 접속과 관련한 비밀번호, IP 주소 등 특정정보를 등록(Hard Coding)할 수 없다.
34. 소스코드에 대한 접근통제 절차를 수립하고 이행하여야 한다.
35. 이전 버전의 소프트웨어는 운영 일시, 지원 소프트웨어, 작업통제, 데이터 정의, 절차 등의 정보와 함께 보관하여야 한다.
36. 웹 응용프로그램 소스와 같이 서비스 특성상 반드시 필요한 경우를 제외하고 모든 응용프로그램 소스는 운영중인 시스템에 저장하여 관리하는 것을 금한다.
37. 개발 중이거나 유지보수 중인 응용프로그램은 운영 중인 응용프로그램의 소스와 분리하여 관리한다.
38. 변경 관리
39. 개발 담당자는 응용프로그램 변경으로 정보보호 기능을 저해해서는 안 된다.
40. 개발 담당자는 개발 중인 프로그램에 대한 버전을 관리하여야 하며, 운영시스템 프로그램 변경버전에 대해 보관 • 관리하여야 한다.
41. 개발 담당자는 변경요청 내역에 관리번호를 부여하여 기록 및 관리하고 정보보호관리자에게 요청사항을 보고한다.
42. 개발 담당자는 응용프로그램 버전 관리와 통제를 위해 형상관리를 수행하여야 한다.
43. 개발 담당자는 변경 수행 완료 후, 관련 내역을 기록∙관리하고 정보보호관리자에게 보고 하여야 한다.
44. 서비스 운영을 위해 긴급한 응용프로그램 변경이 필요하나 정보보호 관리자가 부재한 경우 개발 담당자는 일련의 승인 절차를 생략하고 응용프로그램을 변경할 수 있다.
45. 개발 담당자는 긴급한 응용프로그램 변경 시 변경일자, 변경사유, 변경인력 등을 포함하는 작업내용을 기록∙관리하여야 한다.
46. 정보보호 관리자는 개발 담당자의 긴급 변경 기록 내역을 확인하여 사후 승인하도록 한다.
47. 계정 관리
48. 개발부서는 시스템계정, DB 테이블, 개발 프로그램 등의 권한을 받기 위해서 정보보호최고책임자의 승인을 받아야 한다.
49. 정보보호 관리자는 개발자 별로 접근권한을 설정하고 그 사실을 기록 • 관리해야 한다.
50. 개발을 위해 사용한 임시계정 및 기타 불필요한 계정은 어플리케이션이 오픈 되기 전에 삭제하여야 한다.
51. 개발용 DB 보안 관리
52. 개인 정보를 개발 목적으로 활용하는 것은 원칙적으로 금지되어야 한다. 단, 접근제어 및 암호화 등 운영환경과 동일한 보안통제 하에 제한적으로 사용할 수 있다.
53. 개발부서에서 자체 관리하는 개발용 DB에 대해서는 정보보호 관리자가 응용프로그램 개발 환경의 안정성을 제고하여야 하며 최종적인 보안관리 책임을 가진다. 단, 개인정보를 포함하지 않은 개발용 DB로 한정한다.
54. 정보보호 관리자는 개발용 DB의 계정 생성 현황을 기록∙관리하여야 하고 개발 담당자가 공용 계정을 사용하는 것을 금지한다.
55. 정보보호 관리자는 개발 담당자에게 계정 부여 시 필요한 최소한의 권한을 부여하고 관리∙감독하여야 한다.
56. 폐기 및 기타
57. 사업 부서에서 서비스 중단이 결정되었을 경우 사업 담당자는 사업 관리자의 승인을 거쳐 개발 담당자에게 폐기를 요청하고, 개발 담당자는 정보보호 담당자에게 통보하여야 한다.
58. 개발 담당자는 서버 및 네트워크 담당자에게 서비스 관련 정보시스템의 중단을 요청한다.
59. 외주 개발 보안 관리
60. 개발부서는 어플리케이션 소스 코드의 소유권 및 지적 재산권이 회사에 있음을 외주개발 업체로부터 법적 동의를 받으며 이를 계약서에 명시한다.
61. 개발부서는 외주개발 시 회사로부터 제공된 중요정보의 비밀을 유지해야 하며 이에 대한 요구사항을 계약서에 명시한다.
62. 개발부서는 회사 내에 상주하여 외주개발 시 개발인력은 회사의 정보보호 정책 및 지침을 준수해야 하며 이에 대한 요구사항을 계약서, SLA, 비밀유지서약서 등에 명시한다.(생활보안지침 참조)
63. 개발부서는 아웃소싱업체 대표 및 외주개발자에게 보안서약서를 징구하여야 할 책임이 있다
64. 외주 개발자가 시스템 접근이 필요한 경우 외주 개발자는 시스템 접근요청 메일을 작성하여 개발 담당자를 통해 정보보호 담당자에게 요청하며, 정보보호 담당자는 이를 확인하고 사용자 계정 신청 메일을 작성하여 정보보호 관리자의 승인을 득한 후 계정을 발급한다.
65. 외주 개발자들에게 공동으로 사용하는 계정은 부여하지 않도록 한다. 단 업무상 필요 시 정보보호담당자는 정보보호 관리자에게 메일을 통해 사용자 계정 신청을 요구하여 승인을 받는다.
66. 외주개발 완료 시 정보보호 담당자는 외주 개발자의 계정을 삭제한다.

끝.

**부 칙**

**(시행일)** 이 정책은 2018. 10. 05 부터 시행한다.