[관련문서1]

고유식별정보 안전조치 관리실태 조사 매뉴얼 중(p16~17)

9 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하고 있는지 여부

[점검항목 설명]

개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 **비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷 홈페이지 등에 적용하여야 합니다.**

비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합, 구성하여야 합니다.

특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있습니다.

<비밀번호 작성규칙 예시>

· 비밀번호는 문자, 숫자의 조합.구성에 따라 최소 10자리 또는 8자리 이상의 길이로 설정
  ※ 기술 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있음
  - 최소 10자리 이상: 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개), 특수문자(#, [, ", < 등, 32개) 중 2종류 이상으로 조합.구성한 경우
  - 최소 8자리 이상: 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성한 경우
· 비밀번호는 추측하거나 유추하기 어렵도록 설정
  - 일련번호(12345678 등), 전화번호, 잘 알려진 단어(love, happy 등), 키보드 상에서 나란히 있는 문자열(qwer 등) 등은 사용을 지양
· 비밀번호를 최소 6개월마다 변경하도록 변경기간을 적용하는 등 장기간 사용을 지양
  - 변경 시 동일한(예시: Mrp15@*1aT와 Mrp15@*1at) 비밀번호를 교대로 사용하지 않도록 주의

[점검방법]

비밀번호 작성규칙을 수립하여 적용하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행자부 고시] 개인정보의 안전성 확보조치 기준 제5조(접근권한의 관리)

10 사용자계정 또는 비밀번호를 일정 횟수이상 잘못 입력한 경우, 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는지 여부

[점검항목 설명]

개인정보처리자는 개인정보처리시스템에 권한 없는 자의 비정상적인 접근을 방지하기 위하여 **계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우에는 개인정보처리시스템에 접근을 제한하는 등 기술적 조치를 하여야 합니다.**

계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자계정 잠금 등의 조치를 취하거나 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(공인인증서, OTP 등)을 적용하여 정당한 접근 권한 자임을 확인하는 등의 조치를 취하는 것을 말합니다.

※ 개인정보취급자에게 개인정보처리시스템에 대한 접근을 재 부여하는 경우에도 반드시 개인정보취급자 여부를 확인 후 계정 잠금 해제 등의 조치가 필요

[점검방법]

사용자계정 또는 비밀번호 오 입력 시 개인정보처리시스템에 대한 접근을 제한하는 조치를 취하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행자부 고시] 개인정보의 안전성 확보조치 기준 제5조(접근권한의 관리)

[관련문서2]

개인정보의 안정성 확보조치 기준 고시 해설서 중(p46~47)

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

- 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷 홈페이지 등에 적용하여야 한다.
- 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 한다.

  ※ 비밀번호 이외의 추가적인 인증에 사용되는 휴대폰 인증, 일회용 비밀번호(OTP) 등은 비밀번호 작성규칙을 적용하지 아니할 수 있다.
- 특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다.

TIP · 안전한 비밀번호 설정을 위해 한국인터넷진흥원(KISA)의 암호이용활성화 홈페이지(http://seed.kisa.or.kr)에서 제공하는 "패스워드 선택 및 이용 안내서"나 비밀번호 안전성 검증 소프트웨어 등을 활용할 수 있다.

비밀번호 작성규칙 예시

· 비밀번호는 문자, 숫자의 조합·구성에 따라 최소 10자리 또는 8자리 이상의 길이로 설정

※ 기술 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있다.

- 최소 10자리 이상: 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개), 특수문자(#, [, ", 〈 등, 32개) 중 2종류 이상으로 조합·구성한 경우
- 최소 8자리 이상: 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성한 경우

· 비밀번호는 추측하거나 유추하기 어렵도록 설정

- 일련번호(12345678 등), 전화번호, 잘 알려진 단어(love, happy 등), 키보드 상에서 나란히 있는 문자열(qwer 등) 등을 사용하지 않도록 한다.

· 비밀번호를 최소 6개월마다 변경하도록 변경기간을 적용하는 등 장기간 사용하지 않는다.

- 변경시 동일한(예시: Mrp15@*1aT와 Mrp15@*1at) 비밀번호를 교대로 사용하지 않도록 한다.

⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

- 개인정보처리자는 개인정보처리시스템에 권한 없는 자의 비정상적인 접근을 방지하기 위하여 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우에는 개인정보처리시스템에 접근을 제한하는 등 기술적 조치를 하여야 한다.

  - 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자계정 잠금 등의 조치를 취하거나 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(공인인증서, OTP 등)을 적용하여 정당한 접근 권한자임을 확인하는 등의 조치를 취하는 것을 말한다.

  ※ 개인정보취급자에게 개인정보처리시스템에 대한 접근을 재 부여하는 경우에도 반드시 개인정보취급자 여부를 확인 후 계정 잠금 해제 등의 조치가 필요하다.

[관련문서3]

개인정보 영향평가 수행안내서 중(p288~291)

세부분야	인증 관리				
질의문 코드	질의문	이행	부분이행	미이행	해당없음
4.1.2	○ 개인정보취급자 및 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 적용하도록 계획하고 있습니까?		O		
평가 예시	○ 부분이행 : 비밀번호 설정 시 최소길이(조합도 포함), 동일한 비밀번호 사용제한, 추측 가능한 문자열 포함 제한 등 조합규칙 중 일부만 적용하는 경우				
평가근거 및 의견	○ OO기관의 개인정보취급자의 OO관리시스템 접속 시 계정 비밀번호 설정은 영문, 숫자, 특수문자를 조합하여 8자리 이상의 길이 제한을 하고 있으나, 일련번호, 동일한 비밀번호 사용제한, 일련번호 등의 제한여부는 적용하지 않음				

【주요 점검 사항】

1. 개인정보취급자가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.
   ① 최소 길이 : 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성한 경우 8자리 이상, 2종류 이상으로 구성한 경우 10자리 이상
   ② 변경 주기 : 최소 반기 1회 이상
   ③ 기타 : 추측하기 쉬운 문자·단어 제한(일련번호, 전화번호, 잘 알려진 단어 등), 동일한 비밀번호 재사용 제한 등
2. 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 수립하여 적용해야 한다.
   ※ 단, 정보주체의 편의성 등을 고려하여 자율적으로 적절한 수준을 설정하여 이행
3. 대상기관의 내부 규정(보안지침 등)에 비밀번호 작성규칙이 별도로 명시되어 있다면, 해당 규정도 준수할 수 있도록 해야 한다.

【지표 해설】

○ 안전하지 못한 비밀번호를 사용할 경우 정보가 노출될 위험성이 있다. 안전한 비밀번호란 제3자가 쉽게 추측할 수 없으며 비밀번호 해킹 등을 통해서도 비밀번호를 얻어낼 수 없거나 얻어내는데 많은 시간이 요구되는 것을 의미한다. 따라서 개인정보취급자나 정보주체가 생일, 전화번호 등 추측하기 쉬운 숫자나 문자 등을 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 개인정보처리시스템에 적용하여야 한다.

- 비밀번호 설정·변경 시 입력 값의 자리수와 조합을 체크하여 안전한 비밀번호 작성규칙에 위배되는 경우, 법 위반임을 알리고 작성규칙을 준수토록 하여야 한다.
- 비밀번호의 설정·변경 후 6개월 경과 시 비밀번호 변경 화면을 띄워 비밀번호를 변경할 수 있는 기능을 제공하여야 한다.

○ 비밀번호는 추측하기 어려운 문자와 숫자를 포함하도록 하거나, 전에 사용된 비밀번호를 다시 사용하지 않는 등의 다음과 같은 비밀번호 설정 원칙을 참고하여 생성하도록 한다.

- 비밀번호의 최소 길이 : 비밀번호는 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하여야 하며, 이는 정보주체에 대한 비밀번호 작성규칙과는 달리 반드시 준수하여야 한다(컴퓨터 관련 기술의 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있고, 변경 주기는 짧아질 수 있다.)
  - 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 2종류 이상으로 구성한 경우
  - 최소 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성한 경우

    ※ 특수문자 32개 예시 : ~ ! @ # $ % ^ & * ( ) _ - + = [ ] [ ] | ₩ ; : ' " 〈 〉 , . ? /
- 추측하기 어려운 비밀번호의 생성 :
  - 생성한 비밀번호에 12345678 등과 같은 일련번호, 전화번호 등과 같은 쉬운 문자열이 포함되지 않도록 한다.
  - love, happy 등과 같은 잘 알려진 단어 또는 키보드 상에서 나란히 있는 문자열도 포함되지 않도록 한다.
- 비밀번호의 주기적인 변경 : 비밀번호에 유효기간을 설정하고 적어도 6개월마다 변경함으로써 동일한 비밀번호를 장기간 사용하지 않는다.
- 동일한 비밀번호 사용 제한 : 2개의 비밀번호를 교대로 사용하지 않는다.

○ 비밀번호 작성규칙을 수립한 경우 개인정보취급자 또는 정보주체가 비밀번호를 사용하고자 할 경우 일정 수준 이하의 비밀번호는 설정되지 못하도록 하거나, 주기적으로 패스워드를 변경하지 않을 경우, 시스템 내 사용을 제한하도록 시스템을 통해 자동화 기능을 구현할 수 있다.

○ 개인정보취급자와 달리 정보주체의 비밀번호는 정보주체의 편의성 등을 고려하여 개인정보처리자가 자율적으로 적절한 수준을 설정하는 것이 가능하다. 다만 이 경우에도 정보주체의 편의성만을 고려하여 비밀번호 작성규칙을 전혀 적용하지 않는 것은 바람직하지 않으며, 편의성과 보안성의 균형을 잘 고려하여 최소한의 비밀번호 작성규칙은 적용될 수 있도록 기준을 마련하고 적용할 필요가 있다.

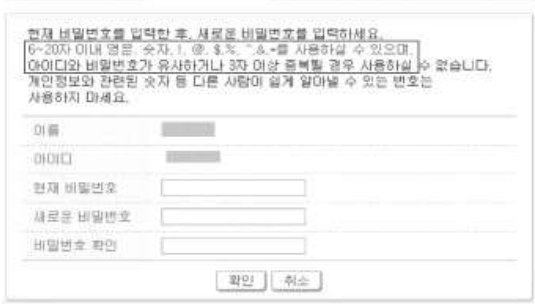
○ 시스템에서 초기에 설정된 디폴트 패스워드는 변경하여 사용하고, 예제 등으로 제시되고 있는 널리 알려진 패스워드는 사용을 금지하여야 한다.

○ 대상 기관이 적용받는 타 법률, 국가정보보안 기본지침 등 상위 기관의 정보보안 지침, 대상 기관 내부의 정보보안 지침 등에서 비밀번호 작성규칙이 명시되어 있다면 해당 지침도 동시에 준수할 수 있도록 비밀번호 작성규칙을 적용할 필요가 있다.

【평가 예시】

구 분	질의문	이행	부분이행	미이행	해당없음
4.1.2	개인정보취급자 및 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 적용하도록 계획하고 있습니까?		○		
평가근거 및 의견	○ OO기관의 개인정보취급자의 OO관리시스템 접속 시 계정 비밀번호 설정은 영문, 숫자, 특수문자를 조합하여 6~20 자리, 아이디와 3자리 이상의 중복여부 등에 대한 조합규칙을 적용하고 있으나, 최소한의 길이가 8자리 이하로 비밀번호 조합규칙의 조건에 미흡하며, 동일한 비밀번호 사용제한 등이 적용되어 있지 않음.				

비밀번호 설정화면



【관련법령 및 문서】

관련 법령 · 지침

【개인정보 보호법】

제23조(민감정보의 처리 제한) ② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.

제24조(고유식별정보의 처리 제한) ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다.

【개인정보 보호법 시행령】

제21조(고유식별정보의 안전성 확보 조치) 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.

제30조(개인정보의 안전성 확보조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정자치부장관이 정하여 고시한다.

【개인정보의 안전성 확보조치 기준 고시】

제4조(접근 권한의 관리) ⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

관련 문서

○ 개인정보 보호법령 및 지침 · 고시 해설서 - 제4장 제29조(안전조치의무)
○ 개인정보의 안전성 확보조치 기준 고시 해설서 - 4. 접근 권한의 관리