2020 고유식별정보 안전조치 관리실태 조사 매뉴얼

[민간부문]

2020년 4월

행정안전부

KISA 한국인터넷진흥원

목 차

1 조사개요

1. 목적

- ㅇ 공공기관 및 5만 명 이상의 고유식별정보처리자 대상, 정기조사를 통해 안전조치 이행 현황을 점검・지원
- ㅇ 고유식별정보처리자의 안전성 확보조치 의무에 대한 경각심을 지속적으로 유지하고, 침해사고에 대한 사전예방 등 선제적 대응체계 마련

2. 조사내용

<table>
<tr><td rowspan="2">조사대상</td><td>공공기관</td><td>민간부문</td></tr>
<tr><td>1. 국회
2. 법원
3. 헌법재판소
4. 중앙선거관리위원회 행정사무 처리기관
5. 중앙행정기관 및 소속기관
6. 지방자치단체(시・도)
7. 지방자치단체(시・군・구)
8. 시 ・ 도 교육청
9. 국가인권위원회
10.「공공기관 운영법」 제4조에 따른 공공기관
11.「지방공기업법」에 따른 지방공사 ・ 공단
12. 특별법에 따라 설립된 특수법인
13. 초・중등교육법, 고등교육법에 따른 각 급 학교</td><td>5만 명 이상 정보주체의
고유식별정보를 처리하는 자</td></tr>
<tr><td>조사주기</td><td colspan="2">2년에 1회 이상</td></tr>
<tr><td rowspan="2">조사항목</td><td colspan="2">고유식별정보(주민등록번호, 운전면허번호, 여권번호, 외국인등록번호) 보유현황</td></tr>
<tr><td colspan="2">고유식별정보에 대한 안전성 확보조치 이행 여부</td></tr>
<tr><td>조사방법</td><td colspan="2">온라인을 통해 고유식별정보 보유현황 및 안전조치 자체점검 결과 등록
※ 결과확인 후 증빙자료(서면) 제출요구 및 검토, 필요시 현장점검</td></tr>
<tr><td>조사기관</td><td colspan="2">행정안전부, 한국인터넷진흥원</td></tr>
</table>

3. 시행근거

개인정보보호법 제24조 제3항~제5항, 시행령 제21조
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. ④ 행정안전부장관은 처리하는 개인정보의 종류・규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제3항에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다. ⑤ 행정안전부장관은 대통령령으로 정하는 전문기관으로 하여금 제4항에 따른 조사를 수행하게 할 수 있다.
제21조(고유식별정보의 안전성 확보 조치) ① 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다. ② 법 제24조제4항에서 "대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다. 1. 공공기관 2. 5만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 자 ③ 행정안전부장관은 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에 대하여 법 제24조제4항에 따라 안전성 확보에 필요한 조치를 하였는지를 2년마다 1회 이상 조사하여야 한다. ④ 제3항에 따른 조사는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에게 온라인 또는 서면을 통하여 필요한 자료를 제출하게 하는 방법으로 한다. ⑤ 법 제24조제5항에서 "대통령령으로 정하는 전문기관"이란 다음 각 호의 기관을 말한다. 1.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제52조에 따른 한국인터넷진흥원(이하 "한국인터넷진흥원"이라 한다) 2. 법 제24조제4항에 따른 조사를 수행할 수 있는 기술적・재정적 능력과 설비를 보유한 것으로 인정되어 행정안전부장관이 정하여 고시하는 법인, 단체 또는 기관

4. 조사절차

①	**대상기관 현황조사 및 시행 안내**
②	**안전조치 이행결과 접수 및 컨설팅**
③	**증빙자료 요구・검토 및 시정요구**
④	**현장점검**

2 참고 및 유의사항

1. 민간부문의 경우, 보건복지 분야의 5만 명 이상 정보주체의 고유식별정보처리자가 '20년 관리실태 조사 대상입니다.

※ 본인인증 과정을 거쳐야 기관현황 등록 및 자체점검을 진행하실 수 있습니다. 기관현황 및 자체점검 결과의 수정 등 원활한 관리를 위해서는 1개 기관당 여러 명의 담당자가 중복하여 등록하는 일이 발생하지 않도록 주의하여 주시기 바랍니다.

☞ 1개 기관당 1명의 담당자가 1개의 결과를 제출

2. 자체점검 결과의 제출일은 '20. 8. 31.(월)입니다.

제출일 전까지는 점검항목별 조치결과에 대한 수정이 가능하오니, 미조치된 사항은 해당 기한까지 조치를 완료하여 반영 부탁드립니다.

☞ 대상기관은 제출일 전까지, 기관현황 및 자체점검 등록을 완료하면 됩니다.

3. 자체점검의 점검항목은「개인정보보호법」및「개인정보의 안전성 확보조치 기준」에 따른 내용입니다.

4. 자체점검 세부항목에서의 "개인정보처리시스템"은 고유식별정보가 포함된 개인정보처리시스템을 말합니다.

5. 자체점검 진행 시 참고자료 목록

- 고유식별정보처리자 안전성 확보조치 관리실태 조사 매뉴얼
- 개인정보의 안전성 확보조치 기준 해설서
- 「개인정보 보호법」해설서
- 표준 개인정보 보호지침
- 개인정보 암호화 조치 안내서
- 공공기관 개인정보 영향평가 수행안내서
- 개인정보 위험도 분석 기준 및 해설서

(개인정보보호 종합포털 → 자료실 → 지침자료에서 다운로드 가능)

6. 관련문의 : 이메일 unique@finss.co.kr, 유선 1800-8671

☞ 관련 문의가 많아 통화가 어려울 수 있으니, 가능하면 이메일을 통하여 문의 부탁드립니다.

3 FAQ

Q1	처리하는 고유식별정보가 없음에도 관리실태 조사대상인가요?

관리실태 조사는 임직원의 고유식별정보까지 포함하여, 민간의 경우 5만 명 이상 정보주체의 고유식별정보를 처리하여야만 조사대상에 해당하나, 공공기관의 경우 개인정보보호법 제24조, 개인정보보호법 시행령 제21조에 근거가 있으며, 임직원의 고유식별정보를 처리하기 때문에 보유량에 따른 기준 없이 개인정보보호법에 따른 공공기관이면 모두 조사 대상에 해당합니다.

Q2	관리실태 조사 대상기관에 해당하는 경우, 기관현황 및 자체점검 결과만 등록하면 되는 것인가요? 그 이후에 추가적으로 해야 하는 것은 없나요?

관리실태 조사 대상기관에 해당할 경우에는, 개인정보보호 종합지원시스템(intra.privacy.go.kr)/개인정보보호 종합포털(privacy.go.kr)에 접속한 후, 고유식별정보 보유현황 등 기관현황에 대한 정보를 등록하고, 안전성 확보조치 이행 여부 확인을 위한 자체점검을 진행하여 결과를 등록하면 됩니다.

대상기관이 기관현황 및 자체점검 결과를 '20.8.31.(월) 까지 등록완료 하였다면, 추가적으로 조치하여야 할 사항은 없습니다.

다만, 대상기관이 제출한 자체점검 결과에 대하여 증빙자료(서면) 요구가 있을 경우에는 이에 대한 대응이 필요합니다.

※ 증빙자료(서면)는 고유식별정보 보유량, 기관규모, 자체점검 결과 등을 고려하여 일부기관 선정 예정 (제출방법 등 관련사항은 9월 이후 개별안내)

Q3	'20.8.31.(월)까지 안전조치 자체점검 결과를 등록하지 않을 경우, 어떠한 처벌을 받게 되나요?

조사기간 내 자체점검 결과 등록을 하지 않은 것에 대한 직접적인 처벌규정은 없습니다.

다만, 조사 대상기관에 해당함에도 불구하고 결과를 제출하지 않은 미제출기관에 대해서는
개인정보보호 현장점검을 통해 안전조치 미비사항이 확인될 경우 과태료 등 행정처분이 과중될 수 있습니다.

Q4	현장점검을 받게 되는 기준은 무엇이며, 언제부터 진행 예정인가요?

현장점검은 관리실태 조사 대상기관 임에도 불구하고 '20.8.31.(월)까지 기관현황 및 자체점검 결과를 등록하지 않은 기관, 대량 고유식별정보 처리기관, 증빙자료 검토결과 시정요구를 받은 기관, 기타 안전조치 미비 기관 등 법 위반 협의가 있다고 인정되는 기관을 대상으로 진행될 예정이며, 점검 일정은 9월부터 12월까지입니다.
다만, 상기 기준 및 일정은 상황에 따라 변동될 수 있습니다.

Q5	대상기관 개인정보보호 담당자로서 기관현황 및 자체점검 결과를 등록하려고 하는데, 소속·부속기관의 수가 많습니다. 소속·부속기관은 상위기관과 별도로 등록하게 할 수는 없는지요?

관리실태 조사 대상기관은 1개 기관당 소속·부속기관의 결과를 포함하여, 1개의 결과를 등록합니다.
소속·부속기관의 고유식별정보 보유량, 시스템 현황, 자체점검 결과 등을 취합·반영하여 '20.8.31.(월)까지 기관현황 및 자체점검 결과등록을 완료하여 주시기 바랍니다.

Q6	**개인정보처리시스템에 있는 고유식별정보뿐만 아니라 일반 종이문서, 업무용 파일에 있는 고유식별정보까지 관리실태 조사대상에 포함되는 것으로 알고 있습니다. 그렇다면 범죄수사 자료나 법원의 소송관련 서류에 포함되어 있는 고유식별정보도 조사대상에 해당하는 것인가요?**

개인정보보호법 시행령 제19조(고유식별정보의 범위)에 따르면 공공기관이 다음의 목적으로 처리하는 고유식별정보의 경우, 개인정보보호법 상 고유식별정보의 범위에서 제외하고 있습니다.

- 다른 법률에서 정한 소관업무를 수행하기 위해 보호위원회의 심의·의결을 거쳐 고유식별정보를 목적 외 용도로 이용하거나 제3자에게 제공하는 경우
- 조약, 그 밖의 국제협정이 이행을 위하여 외국정부 또는 국제기구에 제공하기 위해 처리하는 고유식별정보
- 범죄의 수사와 공소의 제기 및 유지를 위해 처리하는 고유식별정보
- 형(形) 및 감호, 보호처분의 집행을 위하여 처리되는 고유식별정보

이에 따라, 개인정보처리시스템·종이문서·업무용 파일이 위 사항에 해당하는 고유식별정보가 포함되어 있더라도 관리실태 조사에는 해당하지 않습니다.

※ 이외 임직원 고유식별정보 등 위 예외사항에 해당하지 않는 고유식별정보는 모두 조사 대상에 포함

Q7	**고유식별정보가 포함된 개인정보처리시스템 등록 기준은 무엇인가요?** **개인정보처리시스템 보유 기준은 무엇인가요?**

대상기관에서 서버 등을 직접 운영·관리(외부 위탁운영 포함)하는 개인정보처리시스템이 있고, 해당 처리시스템에 고유식별정보가 포함되어 있다면 '기관현황 – 고유식별정보가 포함된 개인정보처리시스템'에 등록하여야 합니다.

이 경우 총 26개 항목에 대하여 점검을 진행하게 되며, 서버 등을 직접 운영·관리(외부 위탁운영 포함)하는 개인정보처리시스템이 없거나, 상위기관에서 운영하는 통합시스템에 접속하여 이용만 하는 경우에는 개인정보처리시스템 '미보유'에 해당하여 총 9개 항목에 대하여 점검을 진행합니다.
(중앙부처에서 배포하였으나 지자체에서 서버를 직접 운영·관리하는 세울 등의 경우, 등록대상)

Q8	**개인정보처리시스템을 2개 이상 보유하고 있을 경우, 1개의 시스템에서는 점검항목에 따른 조치를 완료하였으나, 나머지 1개의 시스템은 미조치라고 가정한다면, 해당 점검항목에 대하여 "조치"로 표시하여야 하나요? "미조치"로 표시하여야 하나요?**

자체점검의 점검항목은 해당 대상기관인 개인정보처리자가 안전성 확보조치 기준을 충실히 이행하고 있는지 확인하기 위한 것으로, '개인정보의 안전성 확보조치 기준은' 개인정보처리시스템의 개수 여부와 관계없이 해당 조치를 이행하도록 의무를 부여하고 있습니다,

2개의 개인정보처리시스템 중 1개의 시스템만 조치하였다면, 해당 점검항목은 "미조치"에 해당합니다.(공공기관의 경우, 소속 및 부속기관이 보유한 처리시스템 포함)
미조치된 시스템에 대하여서는 조치를 완료한 이후 결과를 입력하시는 것이 바람직합니다.

Q9	**기관현황 등록 시 유형 2 또는 유형 3 기준은 어떻게 적용하여야 하나요?** **(유형2 : 10만 명 미만의 정보주체에 관한 개인정보를 보유한 공공기관)** **(유형3 : 10만 명 이상의 정보주체에 관한 개인정보를 보유한 공공기관)**

기관현황 등록시점 기준, 고유식별정보를 포함하여 기관 내에서 보유하고 있는 정보주체에 대한 개인정보 보유량을 의미하는 것으로, 10만 명 미만, 10만 명 이상 등은 보유건수가 아닌 개인정보를 보유하고 있는 정보주체의 수를 말합니다.

<예시>

기관 내에서 10만 명 미만의 개인정보(성명, 주소, 연락처, 고유식별정보 등)를 보유하고 있을 경우

→ 유형2에 해당

하단 그림설명을 참고하시어 유형을 적용하시면 됩니다. (단, 유형1은 점검대상과 관련 없음)

[그림설명 : 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 차등 적용]

Q10	**안전조치 자체점검 시 세부 조치방법 등에 대하여 조사 매뉴얼을 참고하여도 잘 이해가 되지 않아 어려움이 있습니다. 이럴 경우 도움을 얻을 수 있는 방안이 있는지요?**

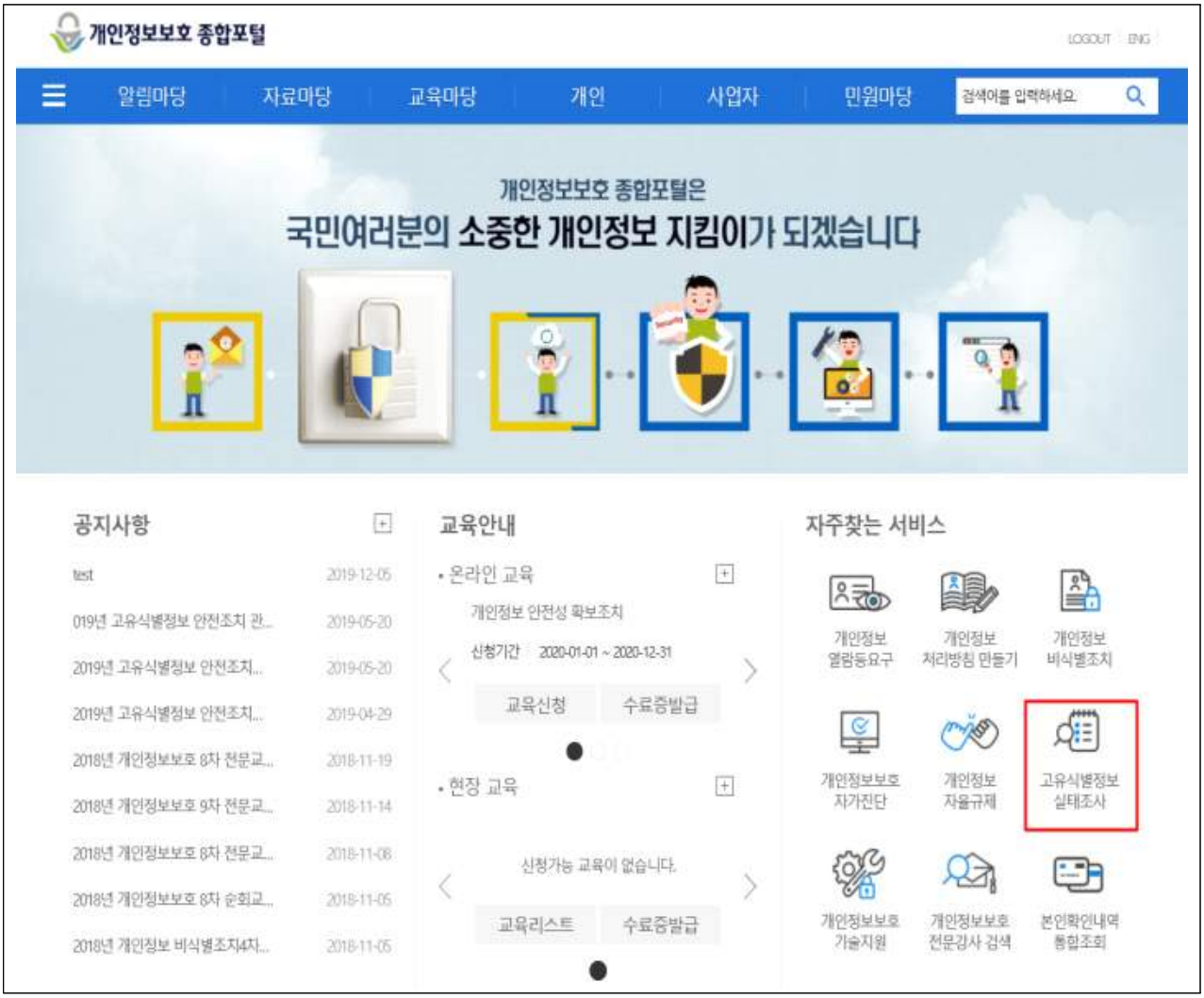
매뉴얼에 기재되어 있는 문의처로 문의하시면 해당 사항에 대한 조치방법 등 상세 안내를 받으실 수 있으며, 기관 내 개인정보보호 관련 전반적인 사항에 대해 도움이 필요하실 경우에는 안전조치 방문 컨설팅을 신청하실 수 있습니다.

※ 문의처 : 고유식별정보 안전조치 관리실태 조사 사무국
(이메일 unique@finss.co.kr, 유선 1800-8671)

※ 방문 컨설팅의 경우 선착순 일부 기관에 한하여 무료로 제공하며, 신청방법은 고유식별정보 안전조치 관리실태 조사 사무국으로 문의

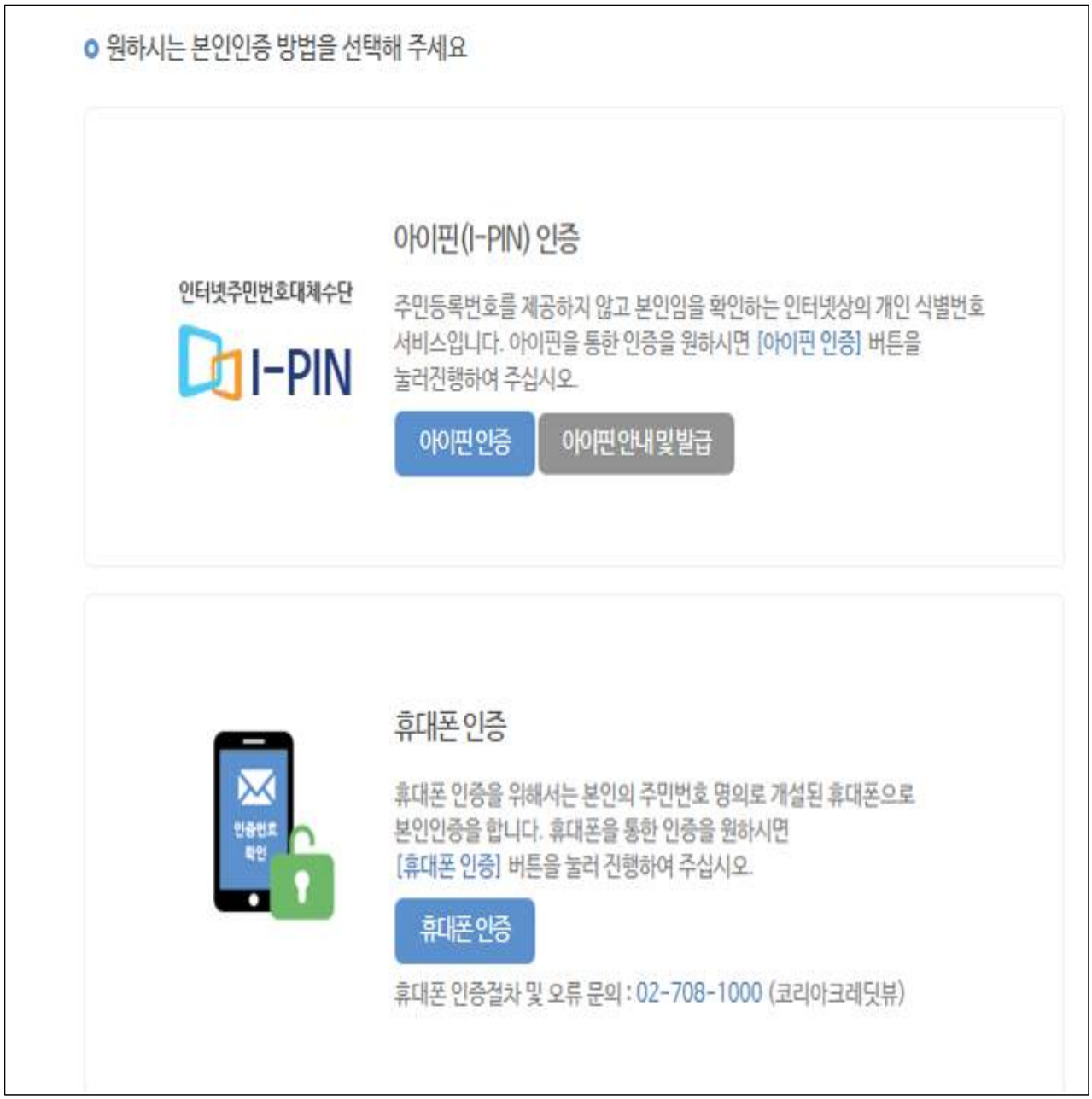
4 시스템 접속

① 개인정보보호 종합포털(https://www.privacy.go.kr)에 접속합니다.
② 메인화면에서 자주 찾는 서비스 "고유식별정보 안전성 확보조치 실태조사" 아이콘을 선택합니다.



③ 고유식별정보 실태조사 안내페이지의 왼쪽 메뉴 중 "기관현황 등록 및 자체점검" 메뉴를 선택합니다.

④ 아이핀 인증 또는 휴대전화 인증을 통하여 본인인증을 합니다.



※ 기관현황 등록 및 자체점검 결과입력은 대상기관별 복수등록이 되지 않으므로, 최초 대상기관의 개인정보 보호 담당자 또는 실태조사 담당자가 본인인증절차 등 관리 실태 조사 관련 사항을 진행할 수 있도록 협조 부탁드립니다.

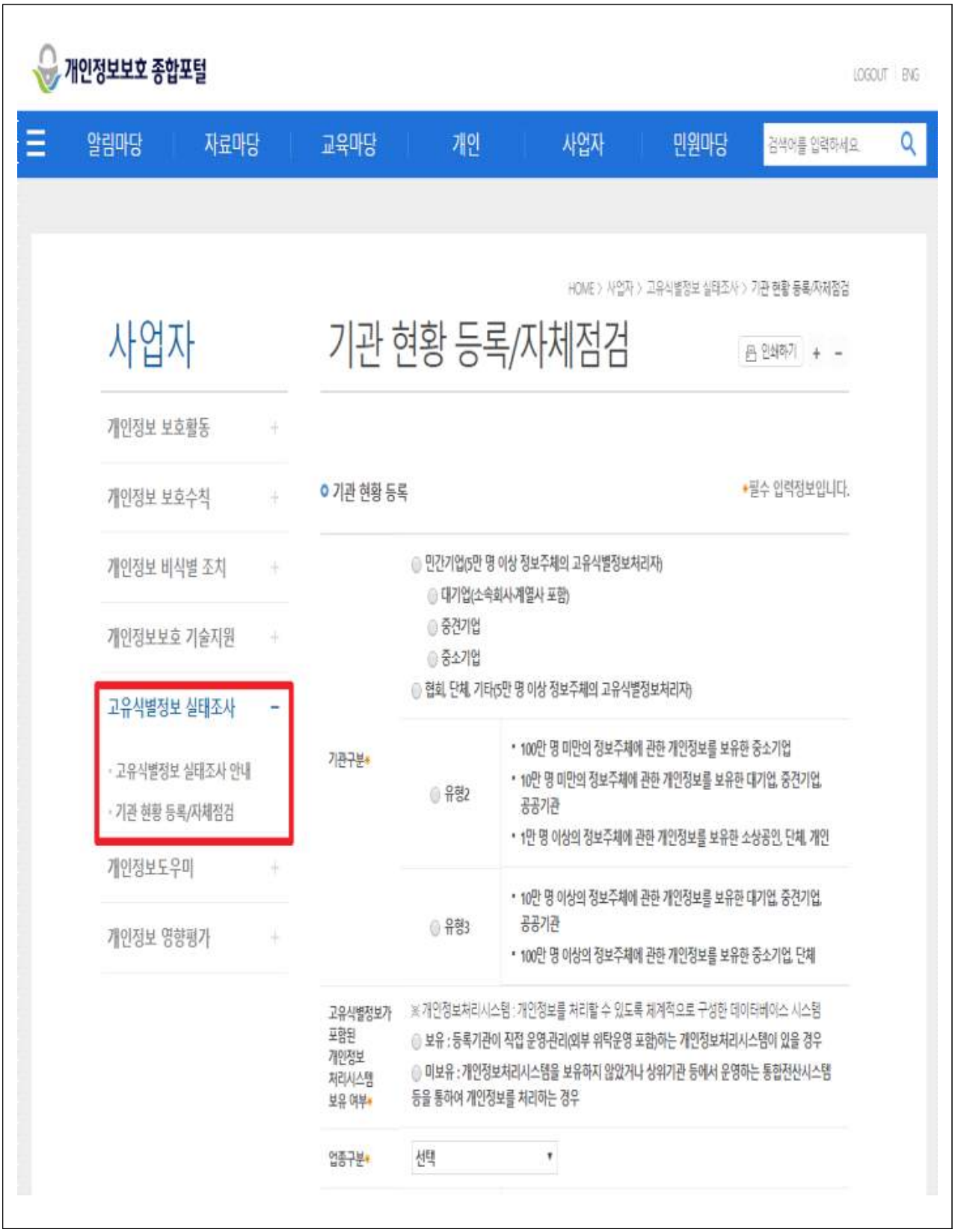
5 기관현황 등록

※ 기관현황 등록사항은 대상기관 담당자 1명이 일괄등록

① 개인정보보호 종합포털(https://www.privacy.go.kr) → 고유식별정보 실태조사(기관현황/자체점검) → 본인인증, 본인인증 절차가 완료되면, 기관현황 등록 페이지로 전환됩니다.

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>1. 개인정보보호 종합포털에서
고유식별정보 바로가기 클릭</td>
<td>2. 고유식별정보 안내페이지에서
기관현황등록/자체점검 클릭</td>
</tr>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>3. 본인인증</td>
<td>4. 기관현황 및 자체점검 작성</td>
</tr>
</table>

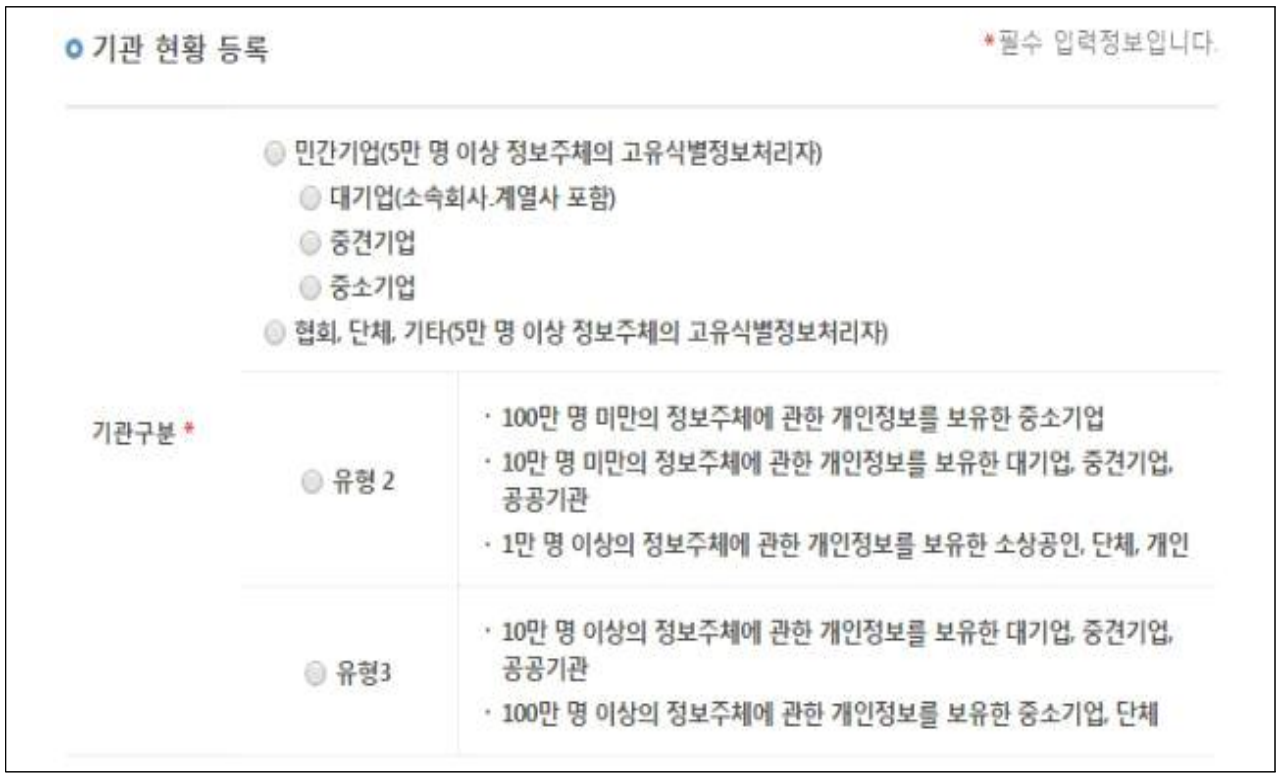
② 자체점검 페이지가 나타나면 기관 세부현황에 대하여 선택하고 관련정보를 입력합니다.



③ 기관구분

: 민간부문에 해당할 경우에는 대기업, 중견기업, 중소기업 중 선택하여 입력하고, 아닐 경우에는 협·단체·기타를 선택합니다.

'유형 2' 또는 '유형 3' 중에서 설명내용에 맞는 유형을 선택합니다.



참고사항

■ 민간부문의 구분('20년 3월 현재기준)

- (대기업, 중견기업, 중소기업) **개인정보의 안전성 확보조치 기준 해설서 20p~23p 참조**

※ 상호출자제한 기업집단(대기업)에 속한 계열회사는 대기업으로 선택하여 입력

■ 유형 2, 유형 3에서의 개인정보 보유량은 고유식별정보를 포함하여 대상기관이 보유하고 있는 정보주체에 대한 개인정보 보유량을 의미하는 것으로, 100만 미만, 10만 미만 등은 보유 건수가 아닌 개인정보를 보유하고 있는 정보주체의 수를 말함

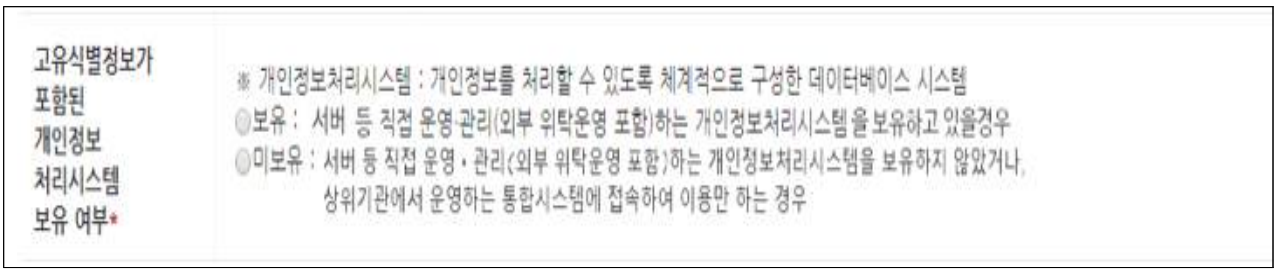
※ 개인정보의 안전성 확보조치 기준

[참고] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준 참조

④ 고유식별정보가 포함된 개인정보처리시스템 보유 여부

: 외부 위탁운영을 포함하여 대상기관에서 직접 운영·관리하는 개인정보처리시스템(서버 등)이 있을 경우에는 '보유'를 선택하여 입력합니다.
상위기관 등에서 운영하는 통합전산시스템 등에 접속하여 이용만 하거나 고유식별정보가 포함된 개인정보처리시스템이 없는 경우에는 '미보유'를 선택하여 입력합니다.

※ 고유식별정보가 포함된 개인정보처리시스템에 대한 보유 여부를 입력



참고사항

■ 개인정보처리시스템이란 일반적으로 데이터베이스(DB) 내의 데이터에 접근할 수 있도록 해주는 응용시스템을 의미하며, 데이터베이스를 구축하거나 운영하는데 필요한 시스템을 말함. 다만, 개인정보처리시스템은 개인정보처리자의 개인정보 처리방법, 시스템 구성 및 운영환경 등에 따라 달라질 수 있음

■ 업무용 컴퓨터의 경우에도 데이터베이스 응용프로그램이 설치.운영되어 다수의 개인정보취급자가 개인정보를 처리하는 경우에는 개인정보처리시스템에 해당될 수 있음 (다만, 데이터베이스 응용프로그램이 설치·운영되지 않는 PC, 노트북과 같은 업무용 컴퓨터는 개인정보처리시스템에서 제외)

⑤ 업종

: 대상기관이 해당하는 업종을 선택하여 입력합니다.

※ 통계청 : 한국표준산업분류의 대분류 참고

o 건설업	o 교육서비스업
o 금융 및 보험업(금융 지원 서비스, 기타 금융, 보험 및 연금관련 서비스, 보험, 신탁 및 집합투자, 연금 및 공제, 은행 및 저축기관)	**o 도매 및 소매업 (도매 및 상품 중개, 소매, 자동차 및 부품 판매)**
o 보건업 및 사회복지 서비스업 (병원, 의원, 사회복지 서비스)	o 사업시설 관리, 사업 지원 및 임대 서비스업 (사업시설 관리 및 조경 서비스, 임대)
o 수도, 하수 및 폐기물 처리, 원료 재생업	o 숙박 및 음식점업(숙박, 음식 및 주점)
o 예술, 스포츠 및 여가관련 서비스업	o 운수 및 창고업(수상 운송, 육상 운송 및 파이프라인 운송, 창고 및 운송관련 서비스, 항공)
o 전기, 가스, 증기 및 공기조절 공급업	o 정보통신업(방송, 영상·오디오 기록물 제작 및 배급, 우편 및 통신, 정보서비스, 출판, 컴퓨터 프로그래밍, 시스템 통합 및 관리)
o 제조업	**o 협회 및 단체, 수리 및 기타 서비스업**

⑥ 기관정보 및 담당자 정보:

기관명(회사명), 사업자등록번호, 대표자명, 회사주소에 대하여 입력합니다.

대상기관 실태조사 담당직원의 부서명, 성명, 회사전화번호, 이메일 주소를 입력합니다.

※ 담당자 정보는 기관현황 및 자체점검 결과에 대한 확인, 향후 진행예정인 현장점검 등 실태조사와 관련한 안내 등을 위하여 필요한 정보이니, 정확하게 기재 부탁드립니다.

⑦ 고유식별정보 보유현황:

대상기관에서 현재 보유하고 있는 고유식별정보의 종류와 건수를 입력합니다.

※ 고유식별정보 보유 건수는 정보주체의 구분 없이 대상기관에서 보유하고 있는 고유식별정보에 대한 총보유량을 기재합니다. (1종 이상 복수선택 가능)

⑧ 고유식별정보가 포함된 개인정보처리시스템 현황:

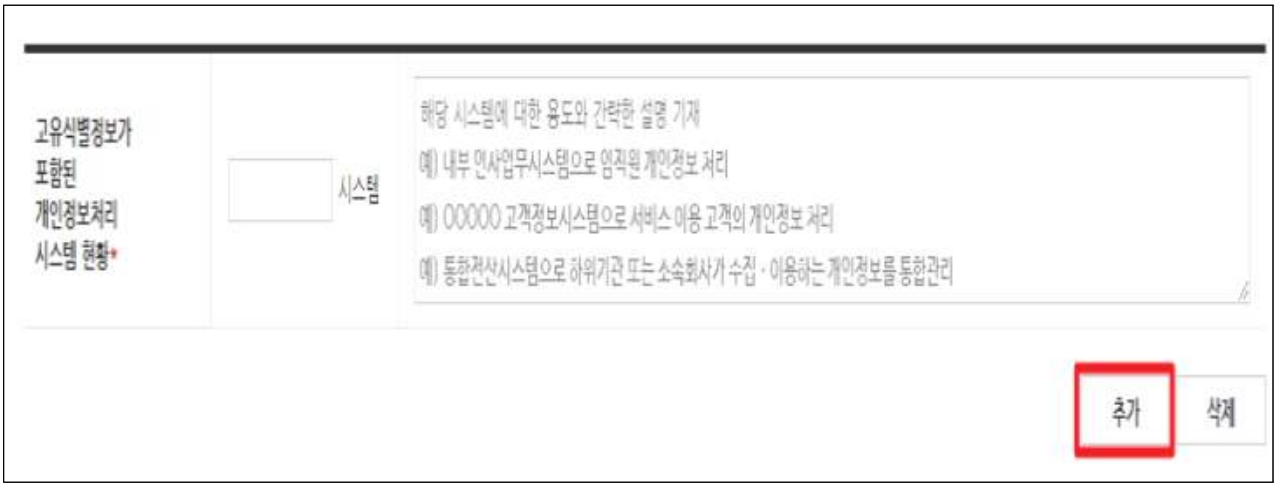
④번 항목에서 개인정보처리시스템 미보유 선택 시에는 비활성화됩니다. 대상 기관이 현재 보유하고 있는 개인정보처리시스템에 대한 명칭과 용도에 대하여 간략하게 기재합니다.

고유식별정보를 단 1건이라도 처리하는 시스템은 개인정보처리시스템으로 등록하며, 보유 여부에 따라 [추가]버튼을 클릭하여 최대 50개까지 등록 가능합니다.

※ 해당 개인정보처리시스템이 50개 이상인 경우, 시스템별 보유량을 기준으로 50개 등록

[예시] OOOO고객정보시스템 : OOOO 고객에 대한 주민등록번호 및 여권번호 처리

[예시] OOOO통합전산시스템 : 산하기관 또는 소속회사에서 처리하는 개인정보를 통합·관리



기관 세부현황에 대한 선택 및 관련정보 입력이 끝나면, [다음] 버튼을 선택해 주세요. ([다음] 버튼을 선택하면 현재까지의 입력정보가 시스템에 저장되며, '자체점검' 화면으로 전환됩니다.)

참고사항

■ 개인정보처리시스템 보유여부(보유·미보유)에 따라 자체점검 항목에 차이가 있으므로, 기관현황 등록이 완료되어야만 자체점검을 진행하실 수 있습니다. 해당 사항에 대하여 충분히 파악한 이후 기관현황 등록을 진행하여 주시기 바라며, **기관현황은 등록이 완료된 이후에도 8월 말 자체점검 결과와 함께 수정이 가능합니다.**

6 점검방법

※ 유형2, 유형3 기준

유형	기준
유형2 (표준)	· 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 · 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인
유형3 (강화)	· 10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체

※ 유형2: 점검항목 19, 26번을 점검하지 않음
※ 유형3: 26가지 항목 모두 점검
※ 개인정보처리시스템 보유 시: 26가지 항목 모두 점검
※ 개인정보처리시스템 미보유 시: 하이라이트 부분 9가지 항목 점검

①	주민등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거가 있는지 여부
②	여권번호, 운전면허번호, 외국인등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거 또는 정보주체의 동의가 있는지 여부
③	수집목적이 달성되었고, 보존기간이 경과한 고유식별정보를 파기하고 있는지 여부
④	개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행하고 있는지 여부 **(유형2일 시 필수항목 12-14번을 포함하지 않을 수 있음)**
⑤	개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는지 여부
⑥	전보 또는 퇴직 등 개인정보취급자 변경 시, 개인정보처리시스템에 대한 접근권한을 변경 또는 말소하고 있는지 여부
⑦	개인정보처리시스템에 대한 개인정보취급자의 접근권한 부여·변경·말소 내역을 기록하고 있으며 3년간 보관하고 있는지 여부
⑧	개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지 않는지 여부
⑨	개인정보취급자 또는 정보주체가 안전한 비밀번호 작성규칙을 수립하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하고 있는지 여부

⑩	사용자계정 또는 비밀번호를 일정 횟수이상 잘못 입력한 경우, 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는지 여부
⑪	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하고 있는지 여부
⑫	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 유출시도를 탐지 및 대응하고 있는지 여부
⑬	외부에서 개인정보처리시스템에 접속 시, 가상사설망(VPN), 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하고 있는지 여부
⑭	개인정보가 인터넷 홈페이지, P2P, 공유설정 등으로 유·노출되지 않도록 개인정보처리시스템, 업무용컴퓨터 등에 접근통제 등에 관한 조치를 하고 있는지 여부
⑮	인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우, 해당 홈페이지에 대해 연 1회 이상 취약점을 점검 및 그에 따른 개선조치를 하고 있는지 여부
⑯	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 개인정보처리시스템에 접속을 차단하고 있는지 여부
⑰	고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는지 여부
⑱	내부망에 고유식별정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는지 여부
⑲	암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립 여부 (유형2일 시 점검하지 않음)
⑳	업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하는지 여부
㉑	개인정보취급자가 개인정보처리시스템에 접속한 기록을 2년 이상 보관·관리하고 있는지 여부
㉒	개인정보취급자가 개인정보처리시스템에 접속한 기록에는 사용자 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행한 업무내용 등이 포함되어 있는지 여부
㉓	악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영 및 최신의 상태로 유지하고 있는지 여부
㉔	개인정보처리시스템에 직접 접속하는 관리용 단말기에 대해 비인가자가 임의로 조작하지 못하도록 조치하고 있는지 여부
㉕	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 장소에 보관하고 있는지 여부
㉖	재해·재난 발생 시, 개인정보의 손실·훼손 등을 방지하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 있는지 여부 (유형2일 시 점검하지 않음)

1	주민등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거가 있는지 여부
관련 규정	**개인정보보호법 제24조의2(주민등록번호 처리의 제한)** **▶ 주민등록번호를 적절한 법령에 따라 처리하는지 여부 확인** 1. 법률・대통령령・국회규칙・대법원규칙・헌법재판소규칙・중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우 3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정안전부령으로 정하는 경우
점검 방법 및 예시	**1. 주민등록번호 처리 여부 확인** 1) 대상기관에서 주민등록번호를 처리(수집・이용・제공 등)하는지 여부를 확인합니다.

진 단 서

등록번호			
연 번 호			
환자의 성명		환자의 주민등록번호	
환자의 주소		(전화번호:)	

**출처 : 의료법 시행규칙[별지 제5호의2서식]*

2. 주민등록번호를 처리하는 적절한 법령을 제시

1) OO법 O조 O항 (고유식별정보의 처리) 등 대상기관의 적절한 법령을 확인합니다.

<법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용하는 경우 예시>

근로기준법 시행령

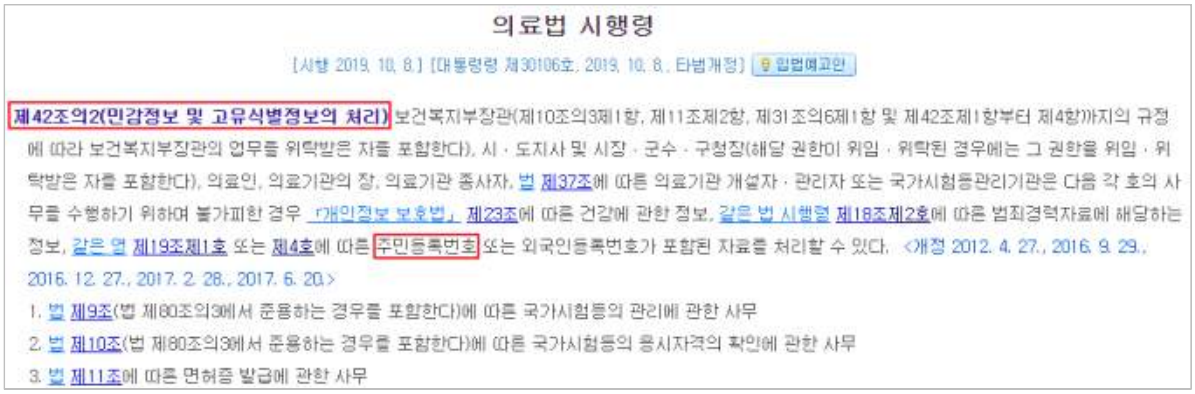
[시행 2020. 3. 3.] [대통령령 제30509호, 2020. 3. 3., 타법개정]

제27조(임금대장의 기재사항) ①사용자는 법 제48조에 따른 임금대장에 다음 각 호의 사항을 근로자 개인별로 적어야 한다.

1. 성명
2. 주민등록번호
3. 고용 연월일
4. 종사하는 업무
5. 임금 및 가족수당의 계산기초가 되는 사항
6. 근로일수
7. 근로시간수
8. 연장근로, 야간근로 또는 휴일근로를 시킨 경우에는 그 시간수
9. 기본급, 수당, 그 밖의 임금의 내역별 금액(통화 외의 것으로 지급된 임금이 있는 경우에는 그 품명 및 수량과 평가총액)
10. 법 제43조제1항 단서에 따라 임금의 일부를 공제한 경우에는 그 금액

점검 방법 및 예시

<법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용하는 경우 예시>



의료법 시행령

[시행 2019. 10. 8.] [대통령령 제30106호, 2019. 10. 8., 타법개정] 입법예고안

제42조의2(민감정보 및 고유식별정보의 처리) 보건복지부장관(제10조의3제1항, 제11조제2항, 제31조의6제1항 및 제42조제1항부터 제4항)까지의 규정에 따라 보건복지부장관의 업무를 위탁받은 자를 포함한다), 시·도지사 및 시장·군수·구청장(해당 권한이 위임·위탁된 경우에는 그 권한을 위임·위탁받은 자를 포함한다), 의료인, 의료기관의 장, 의료기관 종사자, 법 제37조에 따른 의료기관 개설자·관리자 또는 국가시험등관리기관은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강에 관한 정보, 같은 법 시행령 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 같은 영 제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. <개정 2012. 4. 27., 2016. 9. 29., 2016. 12. 27., 2017. 2. 28., 2017. 6. 20.>

1. 법 제9조(법 제80조의3에서 준용하는 경우를 포함한다)에 따른 국가시험등의 관리에 관한 사무
2. 법 제10조(법 제80조의3에서 준용하는 경우를 포함한다)에 따른 국가시험등의 응시자격의 확인에 관한 사무
3. 법 제11조에 따른 면허증 발급에 관한 사무

<주민등록번호 개인정보 수집 근거 예시>

No	분야	법령명	조문명
1	교육분야	고등교육법 시행령	제73조 (고유식별정보의 처리)
2	교육분야	근로자직업능력개발법 시행령	제52조의2 (민감정보 및 고유식별정보의 처리)
3	보건복지	의료법 시행령	제42조의2 (민감정보 및 고유식별정보의 처리)
4	보건복지	응급의료에 관한 법률 시행령	제5조의2 (자료의 범위 등)
5	시설,문화	주택법 시행령	제95조 (고유식별정보의 처리)
6	이동통신분야	전기통신사업법	제32조의4 (이동통신단말장치 부정이용 방지 등)
7	전분야	고용보험법 시행령	제10조 (피보험자 이름 등의 변경 신고)
8	전분야	국가기술자격법 시행령	제26조 (국가기술자격증의 관리 등)
9	전분야	근로기준법 시행령	제27조 (임금대장의기재사항)
10	전분야	진폐의 예방과 진폐근로자의 보호 등에 관한 법률 시행령	제17조의2 (민감정보 및 고유식별정보의 처리)
11	전분야	법인세법	제118조 (주주명부 등의 작성·비치)
12	전분야	부가가치세법	제32조 (세금계산서 등)
13	환경분야	수도법 시행령	제67조의2 (고유식별정보의 처리)
14	환경분야	한강수계 상수원수질개선 및 주민지원 등에 관한 법률 시행령	제30조의3 (고유식별정보의 처리)

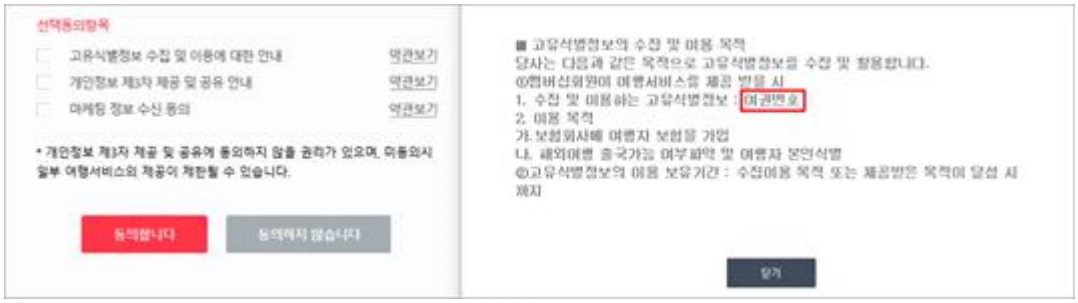
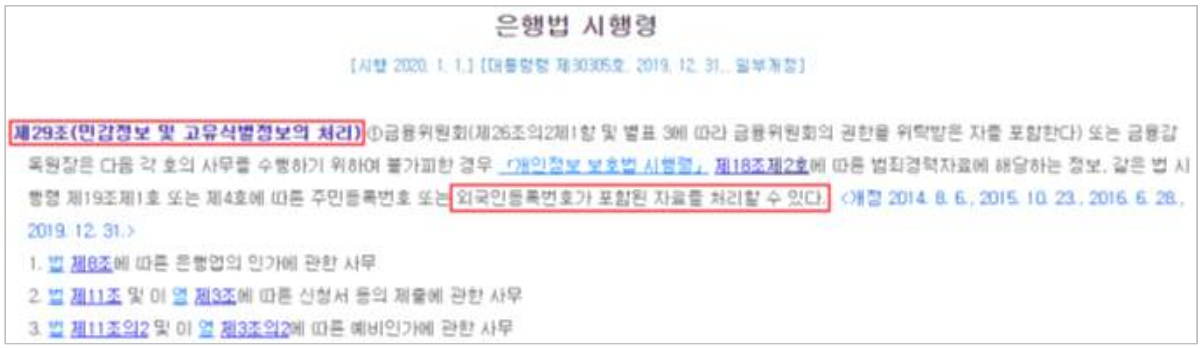
점검 기준

▶ 미조치: 주민등록번호를 처리하나 법령 근거가 없는 경우

▶ 해당없음: 주민등록번호를 처리하지 않는 경우

참고 자료

• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p148~151

<table>
<tr><td>2</td><td>여권번호, 운전면허번호, 외국인등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거 또는 정보주체의 동의가 있는지 여부</td></tr>
<tr><td>관련 규정</td><td>개인정보보호법 제24조(고유식별정보의 처리 제한)
▶ 고유식별정보(여권번호, 운전면허번호, 외국인등록번호)를 적절한 법령에 따라 처리하는지 여부 확인
1. 정보주체에게 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우</td></tr>
<tr><td>점검 방법 및 예시</td><td>1. 고유식별정보(여권번호, 운전면허번호, 외국인등록번호)를 처리할 수 있는 아래의 근거 확인
1) 제15조제2항(정보주체에게 고지하여야 할 4개 항목) 또는 제17조제2항(정보주체에게 고지하여야 할 5개 항목)의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
 
2) 법령에서 고유식별정보의 처리를 요구하거나 허용하는 경우 법적 근거
<법령에서 구체적으로 고유식별정보의 요구하거나 허용하는 경우 예시>
 
은행법 시행령
제29조(민감정보 및 고유식별정보의 처리) ①금융위원회(제26조의2제1항 및 별표 3에 따라 금융위원회의 권한을 위탁받은 자를 포함한다) 또는 금융감독원장은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 같은 법 시행령 제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. <개정 2014. 8. 6., 2015. 10. 23., 2016. 6. 28., 2019. 12. 31.>
1. 법 제8조에 따른 은행업의 인가에 관한 사무
2. 법 제11조 및 이 영 제3조에 따른 신청서 등의 제출에 관한 사무
3. 법 제11조의2 및 이 영 제3조의2에 따른 예비인가에 관한 사무

2. 주민등록번호는 고유식별정보와 분리하여 개인정보보호법 제24조의2(주민등록번호 처리의 제한)에 따라 아래의 근거가 없으면 정보주체의 동의를 받아도 처리할 수 없습니다.
1) 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원 규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2) 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3) 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정안전부령으로 정하는 경우</td></tr>
<tr><td>점검 기준</td><td>▶ 미조치: 고유식별정보를 처리하나 법령 근거가 없거나 정보주체의 별도 동의를 안 받는 경우
▶ 해당없음: 고유식별정보를 처리하지 않는 경우</td></tr>
<tr><td>참고 자료</td><td>• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p144~147</td></tr>
</table>

3 수집목적이 달성되었고, 보존기간이 경과한 고유식별정보를 파기하고 있는지 여부

관련 규정

개인정보보호법 제21조(개인정보의 파기)

▶ 수집목적이 달성되었거나, 보존기간이 지난 고유식별정보 파기 여부 확인

1. 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 개인정보를 파기하여야 함(다만, 법령에 따라 보존해야하는 경우 제외)
2. 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치
3. 개인정보를 파기하지 않고 보존하여야 하는 경우에는 해당 개인정보를 다른 개인정보와 분리하여 저장·관리하여야 한다.

점검 방법 및 예시

1. 개인정보 수집목적에 따른 보유기간을 확인합니다.

1) 수집한 고유식별정보의 보유기간을 확인하고 보유기간이 지난 개인정보가 존재하는지 확인합니다.

<개인정보의 보유기간 예시>

순번	개인정보파일의 명칭	운영근거	보유기간 (목적 달성시)
1	교육서비스 제공 사용자 정보	정보주체 동의	1년
2	개인정보 열람등요구 처리 사용자 정보	개인정보보호법 제35조-제39조	3년
3	유출사고 신고 처리 사용자 정보	개인정보보호법 제34조	3년
4	개인정보보호 전문강사 명단	정보주체 동의	3년

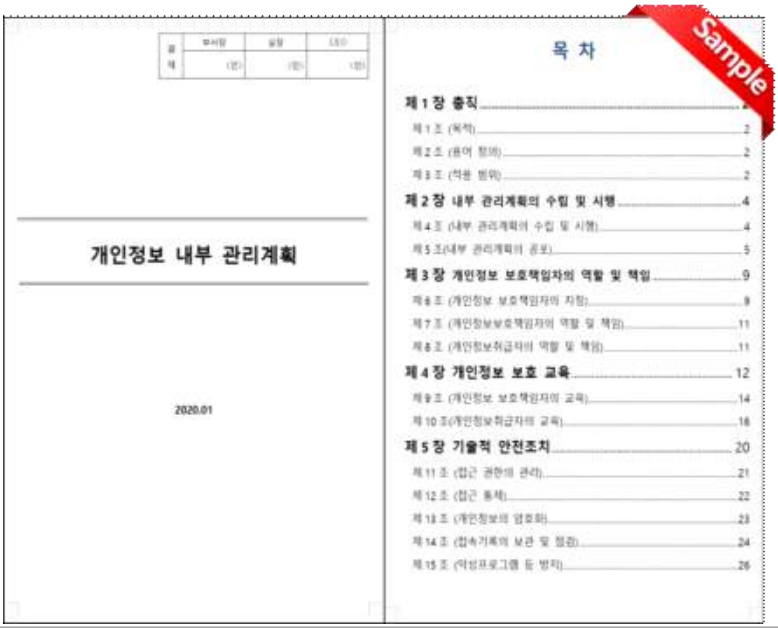
2. 개인정보 파기여부 확인

1) 개인정보 보유기간이 경과된 경우 보유기간 종료일로부터 지체없이 파기를 수행하고 있는지 확인합니다.
2) 파기수행에 대한 증적은 개인정보파일 파기 관리대장을 통해 관리합니다.
3) 다만, 법령에 따라 보존하여야 하는 경우 기존 개인정보파일과 분리하여 별도 보관하여야 합니다.

<보존의무를 규정하고 있는 입법례>

「전자상거래 등에서의 소비자보호에 관한 법률」제6조 및 동시행령 제6조	① 표시·광고에 관한 기록 : 6개월 ② 계약 또는 청약철회 등에 관한 기록 : 5년 ③ 대금결제 및 재화등의 공급에 관한 기록 : 5년 ④ 소비자의 불만 또는 분쟁처리에 관한 기록 : 3년

<table>
<tr><td>점검
방법
및
예시</td><td>
<보존의무를 규정하고 있는 입법례>
<table>
<tr><td>「의료법」제22조제2항
및 동시행령 제15조</td><td>① 환자 명부: 5년
② 진료기록부: 10년
③ 처방전 : 2년
④ 수술기록 : 10년
⑤검사내용 및 검사소견기록 : 5년
⑥방사선 사진(영상물) 및 그 소견서 : 5년
⑦간호기록부 : 5년
⑧조산기록부 : 5년
⑨진단서 등의 부본 : 3년</td></tr>
</table>
</td></tr>
<tr><td>점검
기준</td><td>▶ 미조치: 보유기간이 지난 고유식별정보가 존재하는 경우
▶ 해당없음: 없음</td></tr>
<tr><td>참고
자료</td><td>• 행정안전부, “개인정보보호 법령 및 지침·고시 해설(2016.12.)”, p120~126</td></tr>
</table>

4	개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립 · 시행)** **▶ 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 필수사항을 포함하는 내부 관리계획을 수립·시행하는지 여부 확인** ※ 유형2일 시 필수항목 12-14번을 포함하지 않을 수 있음
점검 방법 및 예시	**1. 내부관리계획 시행 여부 확인** 1) 개인정보의 안전한 처리를 위해 개인정보책임자의 의무와 책임, 개인정보 처리단계별 기술적·관리적 안전조치, 개인정보 교육, 개인정보 침해대응 및 피해구제 등과 같은 개인정보보호 의무를 위한 내부 관리계획서 수립 · 시행 여부 확인합니다. <개인정보 내부관리계획 예시>  <내부관리계획 필수사항> 1. 개인정보 보호책임자의 지정에 관한 사항 2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 3. 개인정보취급자에 대한 교육에 관한 사항 4. 접근 권한의 관리에 관한 사항 5. 접근통제에 관한 사항 6. 개인정보의 암호화 조치에 관한 사항 7. 접속기록 보관 및 점검에 관한 사항 8. 악성프로그램 등 방지에 관한 사항 9. 물리적 안전조치에 관한 사항 10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항 11. 개인정보 유출사고 대응 계획 수립 · 시행에 관한 사항 12. 위험도 분석 및 대응방안 마련에 관한 사항 13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항 14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 15. 그 밖에 개인정보 보호를 위하여 필요한 사항

점검 방법 및 예시

2) 내부관리계획이라는 명칭 이외의 다른 명칭(예: 개인정보 보호지침 등)으로 수립하여도 내부관리계획의 필수반영사항(14개) 사항이 모두 포함된 경우 내부관리계획으로 인정됩니다.

유형	개인정보처리자 유형	수립여부
유형2 (표준)	100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	수립
유형3 (강화)	10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체	수립

점검 기준

▶ 미조치: 내부관리계획을 수립하지 않거나 유형에 따른 필수항목이 누락된 경우
▶ 해당없음: 없음

참고 자료

• 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p34~46
• 개인정보보호 종합포털 > 공지사항 > "개인정보보호 전문교육 교재(내부관리계획)" 참조
(https://www.privacy.go.kr/edu/ttb/selectBoardArticle.do?nttId=1434&bbsId=BBSMSTR_000000000032)

5	개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)** ▶ **개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는지 확인** 1. 업무 성격에 따라 접근 권한을 팀별, 개인정보취급자별 차등 부여 여부 확인 2. 업무처리 방법(조회, 생성, 변경 삭제 등)에 따라 접근권한 부여 여부 확인 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 해당 기관의 개인정보취급자 식별** 1) 개인정보처리시스템에 접근 가능한 개인정취급자를 식별합니다. **2. 기관 내 식별된 개인정보취급자의 담당업무에 적합한 개인정보처리시스템 접근권한 부여 확인** 1) 식별된 개인정보취급자의 업무 목적에 적합하게 최소한의 범위로 접근권한이 부여되어 있는지 접근권한관리 테이블, 접근권한 관리대장 등을 확인합니다.
점검 기준	▶ 미조치: 개인정보처리시스템 접근권한을 차등 부여하지 않을 경우 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p210 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p47~48

개인정보처리시스템 접근권한 관리대장

순번	부서	사용자	계정	업무	접근권한	변경일시	변경사유	처리자
1	인사팀	홍팀장	hong123	인사관리	인사정보(입력, 조회, 수정, 삭제)	2017-03-24, 15:00	입사	김이사
2	인사팀	박대리	assi05	인사관리	인사정보(입력, 조회, 수정)	2017-05-05, 15:00	입사	김이사
3	인사팀	최인턴	inte111	인사관리	인사정보(입력)	2020-02-03, 10:00	입사	김이사
4	영업팀	김팀장	kim112	영업관리	영업정보(입력, 조회, 수정, 삭제)	2017-07-31, 15:00	입사	김이사
5	영업팀	박대리	assi05	영업관리	영업정보(입력, 조회)	2020-03-01, 10:00	부서변경	김이사
6	영업팀	나직원	staff01	-	-	2020-03-24, 15:00	퇴직	김이사
7	정보팀	한팀장	han122	전산관리	인사정보(입력, 조회, 수정, 삭제), 영업정보(입력, 조회, 수정, 삭제)	2017-04-02, 15:00	입사	김이사
8	정보팀	주대리	joo890	전산관리	인사정보(입력, 조회, 수정), 영업정보(입력, 조회, 수정)	2017-05-05, 15:00	입사	김이사
9	정보팀	이사원	empl777	전산관리	인사정보(입력, 조회), 영업(입력, 조회)	2018-10-10, 09:00	입사	김이사

6 전보 또는 퇴직 등 개인정보취급자 변경 시, 개인정보처리시스템에 대한 접근권한을 변경 또는 말소하고 있는지 여부

관련 규정

개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)

▶ **개인정보취급자의 전보 또는 퇴직 등 인사이동 발생 시 개인정보처리시스템의 접근권한을 즉시 변경 또는 말소하는지 확인**

1. 직원의 퇴직 시 해당 직원의 계정을 지체없이 변경·말소하는 조치 등을 내부 관리계획 등에 반영하여 이행하도록 함
2. 직원의 퇴직 시 계정 말소를 효과적으로 이행하기 위해서는 퇴직 점검표에 사용자계정의 말소 항목을 반영하여, 계정 말소 여부에 대해 확인

※ 개인정보처리시스템 미보유 시 점검하지 않음

점검 방법 및 예시

1. 내부관리계획 내 접근권한 관리 반영

1) 개인정보 내부관리계획에 접근권한의 변경·말소에 관한 사항을 반영하여 수립·시행하고 있는지 확인합니다.

2. 인사이동이 확인된 개인정보취급자에 대한 접근권한 변경 말소 내역 확인

1) 조직 내의 임직원의 전보 또는 퇴직, 휴직 등 인사이동이 발생하여 사용자계정의 변경·말소 등이 필요한 경우에는 사용자계정 관리절차에 따라 통제합니다.

개인정보처리시스템 접근권한 관리대장

순번	부서	사용자	계정	업무	접근권한	변경일시	변경사유	처리자
1	인사팀	홍팀장	hong123	인사관리	인사정보(입력, 조회, 수정, 삭제)	2017-03-24, 15:00	입사	김이사
2	인사팀	박대리	assi05	인사관리	인사정보(입력, 조회, 수정)	2017-05-05, 15:00	입사	김이사
3	인사팀	최인턴	inte111	인사관리	인사정보(입력)	2020-02-03, 10:00	입사	김이사
4	영업팀	김팀장	kim112	영업관리	영업정보(입력, 조회, 수정, 삭제)	2017-07-31, 15:00	입사	김이사
5	영업팀	박대리	assi05	영업관리	영업정보(입력, 조회)	2020-03-01, 10:00	부서변경	김이사
6	영업팀	나직원	staff01	-	-	2020-03-24, 15:00	퇴직	김이사
7	정보팀	한팀장	han122	전산관리	인사정보(입력, 조회, 수정, 삭제), 영업정보(입력, 조회, 수정, 삭제)	2017-04-02, 15:00	입사	김이사
8	정보팀	주대리	joo890	전산관리	인사정보(입력, 조회, 수정), 영업정보(입력, 조회, 수정)	2017-05-05, 15:00	입사	김이사
9	정보팀	이사원	empl777	전산관리	인사정보(입력, 조회), 영업(입력, 조회)	2018-10-10, 09:00	입사	김이사

2) 계정 말소를 효과적으로 이행하기 위해서 퇴직 및 인사이동 점검표에 사용자 계정 말소 항목을 반영하여, 계정 말소에 대한 확인을 받을 수 있습니다.

퇴직 및 인사이동 점검표

순번	날짜	사용자	계정	퇴직/인사이동	정변경/계정말	처리자
1	2020.03.01.	박대리	assi05	인사이동(인사팀->영업팀)	변경	김이사
2	2020.03.24.	나직원	staff01	퇴직	말소	김이사

점검 기준

▶ 미조치: 퇴직 및 인사이동 후 개인정보처리시스템 접근권한 변경 말소·미 적용 시

▶ 해당없음: 없음

참고 자료

- 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p210
- 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p47~48

7	개인정보처리시스템에 대한 개인정보취급자의 접근권한 부여·변경·말소 내역을 기록하고 있으며 3년간 보관하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)** ▶ **개인정보취급자의 접근권한 부여 및 전보 또는 퇴직에 따른 변경, 말소에 대한 기록은 최소 3년간 보관하고 있는지 확인** 1. 개인정보처리자는 접근권한 부여·변경·말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관 2. 신청자 정보, 신청일시, 승인자 및 발급자 정보, 신청 및 발급 사유 등 접근권한의 발급 과정과 이력 등을 확인할 수 있도록 필요한 정보를 보관 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 해당 개인정보처리시스템 구축 이후 최소 3년간 접근권한 부여, 변경, 말소 내역 기록여부 확인** 1) 해당 개인정보처리시스템에 접근권한변경 기록이 구축 이후 최소 3년간 기록되고 있는지 확인합니다. <접근권한 변경 기록을 3년 이상 보관 예시>
점검 기준	▶ 미조치: 개인정보취급자의 접근권한 부여·변경·말소 내역을 기록하지 않거나 3년간 미보유 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p210 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p47~48

개인정보처리시스템 접근권한 관리대장

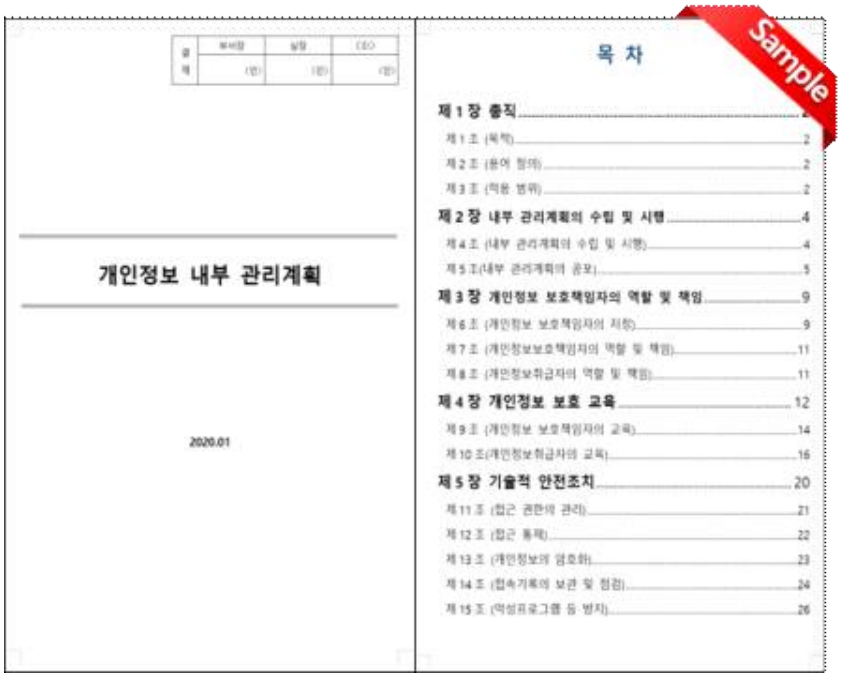
순번	부서	사용자	계정	업무	접근권한	변경일시	변경사유	처리자
1	인사팀	홍팀장	hong123	인사관리	인사정보(입력, 조회, 수정, 삭제)	2017-03-24, 15:00	입사	김이사
2	인사팀	박대리	assi05	인사관리	인사정보(입력, 조회, 수정)	2017-05-05, 15:00	입사	김이사
3	인사팀	최인턴	inte111	인사관리	인사정보(입력)	2020-02-03, 10:00	입사	김이사
4	영업팀	김팀장	kim112	영업관리	영업정보(입력, 조회, 수정, 삭제)	2017-07-31, 15:00	입사	김이사
5	영업팀	박대리	assi05	영업관리	영업정보(입력, 조회)	2020-03-01, 10:00	부서변경	김이사
6	영업팀	나직원	staff01	-	-	2020-03-24, 15:00	퇴직	김이사
7	정보팀	한팀장	han122	전산관리	인사정보(입력, 조회, 수정, 삭제), 영업정보(입력, 조회, 수정, 삭제)	2017-04-02, 15:00	입사	김이사
8	정보팀	주대리	joo890	전산관리	인사정보(입력, 조회, 수정), 영업정보(입력, 조회, 수정)	2017-05-05, 15:00	입사	김이사
9	정보팀	이사원	empl777	전산관리	인사정보(입력, 조회), 영업(입력, 조회)	2018-10-10, 09:00	입사	김이사

8	개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지 않는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)** ▶ **개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 취급자 별로 한 개의 사용자 계정을 발급하고 다수의 사용자가 공유하는지 여부 확인** 1. 개인정보처리시스템에 접속할 수 있는 사용자계정은 개인정보취급자별로 발급 2. 다른 개인정보취급자와 공유되지 않도록 하여야 함 3. 다수의 개인정보취급자가 동일한 업무를 수행한다 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임 추적성을 확보 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 해당 기관의 개인정보취급자 식별** 1) 개인정보처리시스템에 접근 가능한 개인정보취급자를 식별합니다. **2. 기관 내 식별된 개인정보취급자별 개별 계정 발급 여부 확인** 1) 개인정보처리시스템에 접속할 수 있는 사용자 계정이 개인정보취급자별로 발급되었는지 확인합니다. 2) 발급된 계정을 여러 사람이 공유되지 않는지 확인합니다.
점검 기준	▶ 미조치: 사용자계정을 다른 개인정보취급자 등과 공유 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p210 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p47~49

개인정보처리시스템 접근권한 관리대장

순번	부서	사용자	계정	업무	접근권한	변경일시	변경사유	처리자
1	인사팀	홍팀장	hong123	인사관리	인사정보(입력, 조회, 수정, 삭제)	2017-03-24, 15:00	입사	김이사
2	인사팀	박대리	assi05	인사관리	인사정보(입력, 조회, 수정)	2017-05-05, 15:00	입사	김이사
3	인사팀	최인턴	inte111	인사관리	인사정보(입력)	2020-02-03, 10:00	입사	김이사
4	영업팀	김팀장	kim112	영업관리	영업정보(입력, 조회, 수정, 삭제)	2017-07-31, 15:00	입사	김이사
5	영업팀	박대리	assi05	영업관리	영업정보(입력, 조회)	2020-03-01, 10:00	부서변경	김이사
6	영업팀	나직원	staff01	-	-	2020-03-24, 15:00	퇴직	김이사
7	정보팀	한팀장	han122	전산관리	인사정보(입력, 조회, 수정, 삭제), 영업정보(입력, 조회, 수정, 삭제)	2017-04-02, 15:00	입사	김이사
8	정보팀	주대리	joo890	전산관리	인사정보(입력, 조회, 수정), 영업정보(입력, 조회, 수정)	2017-05-05, 15:00	입사	김이사
9	정보팀	이사원	empl777	전산관리	인사정보(입력, 조회), 영업(입력, 조회)	2018-10-10, 09:00	입사	김이사

<개인정보취급자별 개별 계정 부여 예시>

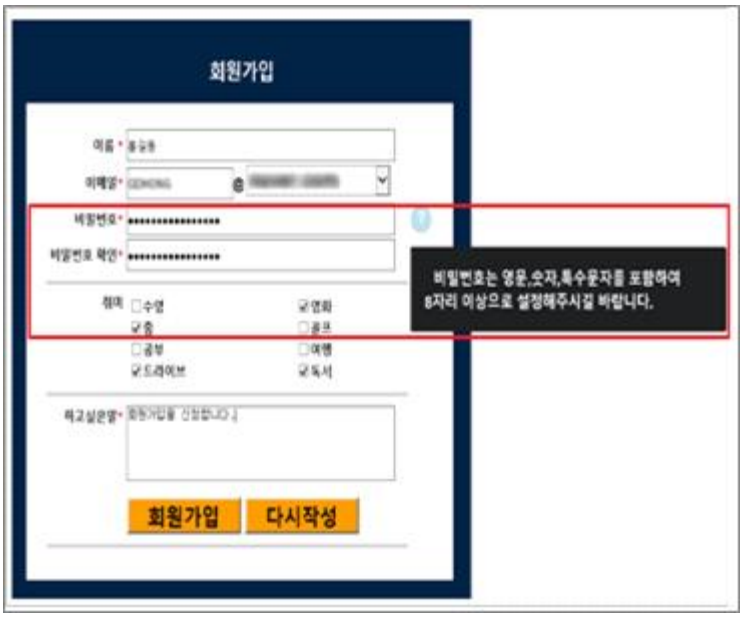
9	개인정보취급자 또는 정보주체가 안전한 비밀번호 작성규칙을 수립하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)** **▶ 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립·적용하는지 확인** 1. 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷 홈페이지 등에 적용 2. 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합, 구성 ※ 비밀번호 이외의 추가적인 인증에 사용되는 휴대폰 인증, 일회용 비밀번호(OTP) 등은 비밀번호 작성규칙을 적용하지 아니할 수 있다. ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 안전한 비밀번호 작성규칙의 수립여부 확인** 1) 개인정보처리시스템 접근 시 개인정보취급자, 서비스 이용자 전체에 대하여 안전한 비밀번호 작성규칙을 적용하도록 패스워드 작성규칙을 수립하고 있는지 확인합니다. 2) 패스워드 작성규칙 수립은 내부관리계획에 포함될 수도 있으며, 개인정보보호 정책/지침 혹은 정보보안 정책/지침에 수립될 수 있습니다. <개인정보 내부관리계획 예시> 

점검 방법 및 예시

2. 수립된 비밀번호 작성규칙 실제 시스템 적용 확인

1) 관련 지침을 통해 수립한 패스워드 작성규칙을 실제 개인정보처리시스템에 적용·이행하고 있는지 확인합니다.

<비밀번호 작성 규칙 적용 예시>



<비밀번호 작성규칙 권장사항>

· **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), 키보드상에서 나란히 있는 문자열(qwer 등) 등은 사용을 지양

· **비밀번호를 최소 변경기간을 적용하는 등 장기간 사용을 지양**

- 변경 시 동일한(예시: Mrp15@*1aT와 Mrp15@*1at) 비밀번호를 교대로 사용하지 않도록 주의

점검 기준

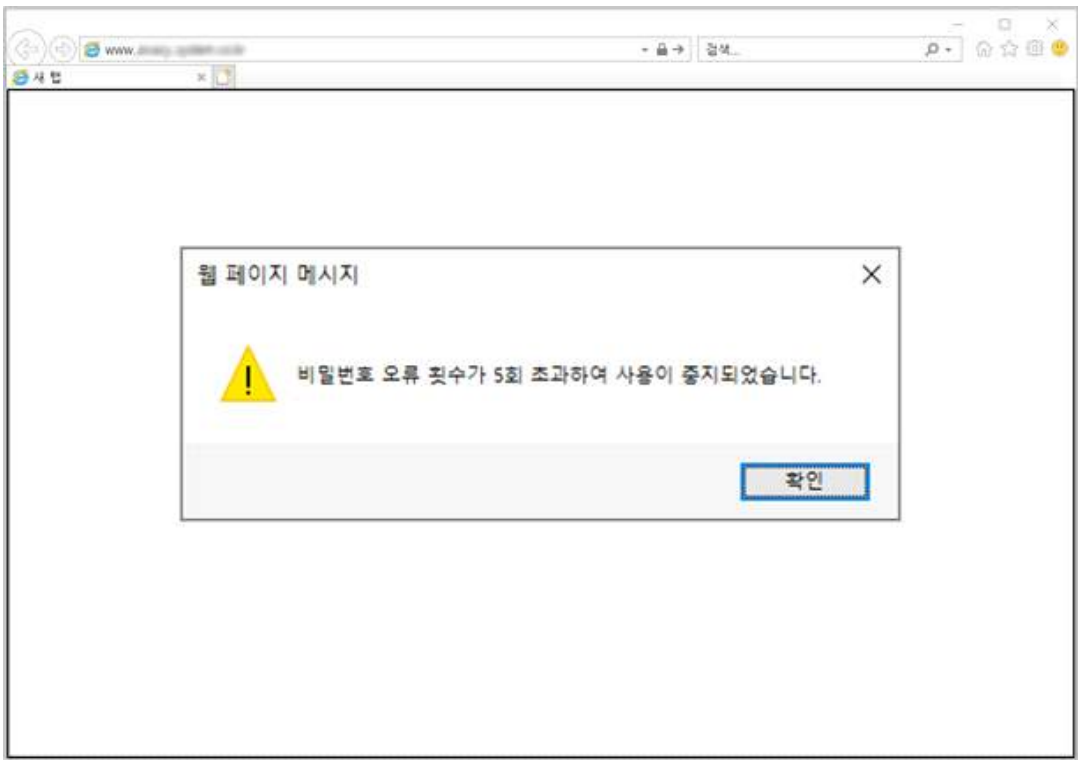
▶ 미조치: 비밀번호 작성규칙 미수립 및 미적용 시

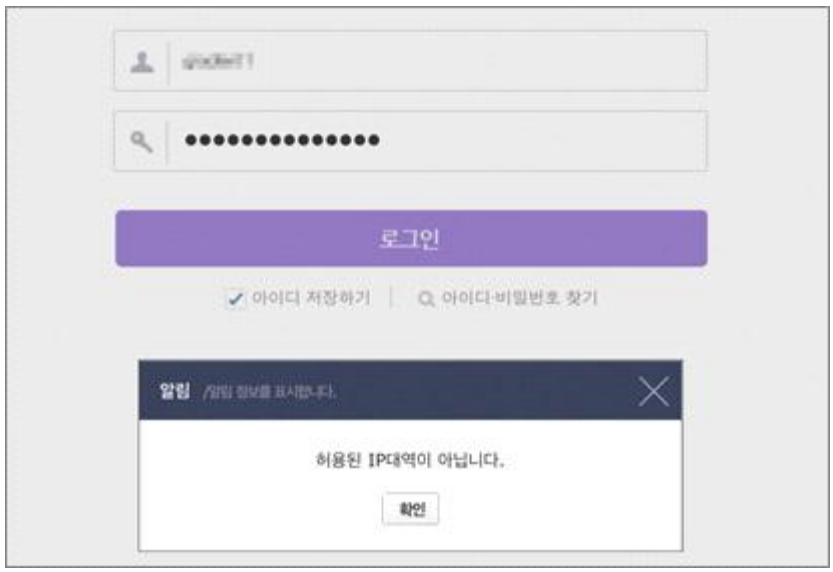
▶ 해당없음: 없음

참고 자료

• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p210~211

• 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p47~50

10	사용자계정 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우, 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)** ▶ **개인정보취급자 또는 정보주체가 계정에 대한 비밀번호를 일정 횟수 이상 잘못 입력하는 경우 접근 제한 여부 확인** 1. 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 사용자계정 잠금 등의 조치 2. 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(공인인증서, OTP 등)을 적용하여 정당한 접근 권한 자임을 확인하는 등의 조치 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 비밀번호 입력 횟수 제한 여부 확인** 1) 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는지 여부를 확인합니다. ※ 개인정보취급자에게 개인정보처리시스템에 대한 접근을 재부여하는 경우에도 반드시 개인정보취급자 여부를 확인 후 계정 잠금 해제 등의 조치가 필요합니다. <비밀번호 오입력에 따른 접근 제한 예시> 
점검 기준	▶ 미조치: 비밀번호 입력 횟수 제한 미적용 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p211 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p47~50

11	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제6조(접근통제)** **▶ 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하고 있는지 여부** 1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 개인정보처리시스템 접근통제 확인** 1) 운영 중인 개인정보처리시스템(DB, 웹, WAS, PC 등)에 지정된 IP, 등록된 ID만 접근할 수 있도록 설정되어 있는지 확인 2) 개인정보처리시스템 자체에서 이를 설정할 수 없을 경우 해당 시스템까지 경유하기까지 보안장비에 대한 룰 설정값 확인(개인정보처리시스템에 대한 접근을 특정 IP만 접근 가능하도록 통제) 3) 개인정보처리시스템에 대한 접속 권한을 IP(Internet protocol)주소, 포트(Port), MAC(Media Access Control) 주소 등으로 제한하여 인가받지 않은 접근을 제한하는지 확인 4) 업무 PC에 문서파일로 개인정보를 보관하고 있을 경우 반드시 해당 PC에 지정된 개인정보 취급자에 한하여 사용자인증(ID/PW) 단계를 거친 후 PC를 이용할 수 있도록 함 <개인정보처리시스템 IP제한 설정>  <IP접근제어 예시> 

점검 방법 및 예시

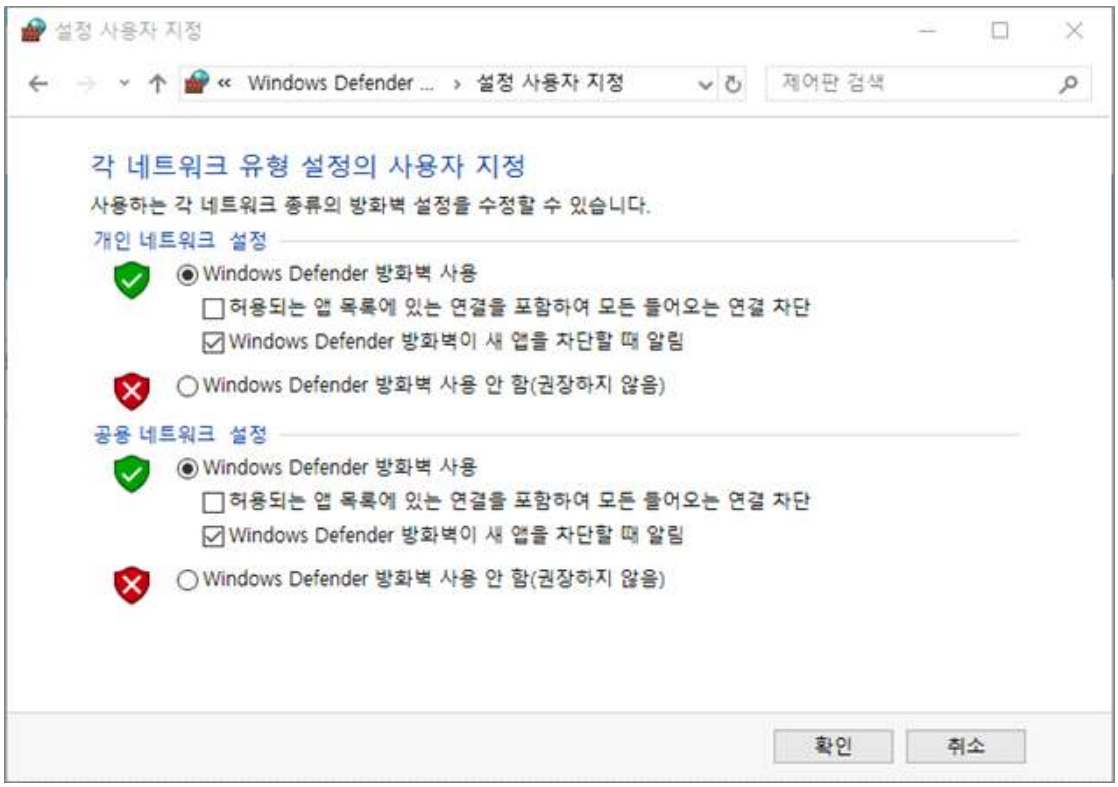
2. 업무용 컴퓨터 또는 모바일 기기에 접근통제 기능 사용 여부 확인

1) 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우, 해당 기기의 운영체제(OS)에서 제공하는 접근통제 기능(방화벽 설정 등) 또는 별도의 보안프로그램을 이용하여 접근통제를 실시할 수 있음

※ PC, 노트북 등의 업무용 컴퓨터의 운영체제(OS)에서 제공하는 접근통제 기능 설정 방법
(업무용 컴퓨터 : 제어판 ->Windows 방화벽 ->Windows 방화벽 설정 또는 해제)

2) 모바일 기기에서는 불필요한 네트워크 소프트웨어 통제, 인입 포트 차단 등의 접근통제 기능을 제공하는 운영체제(OS)를 사용할 수 있으며, 별도의 방화벽 등의 어플리케이션을 설치, 운영이 필요할 수 있음

<윈도우 방화벽 설정>



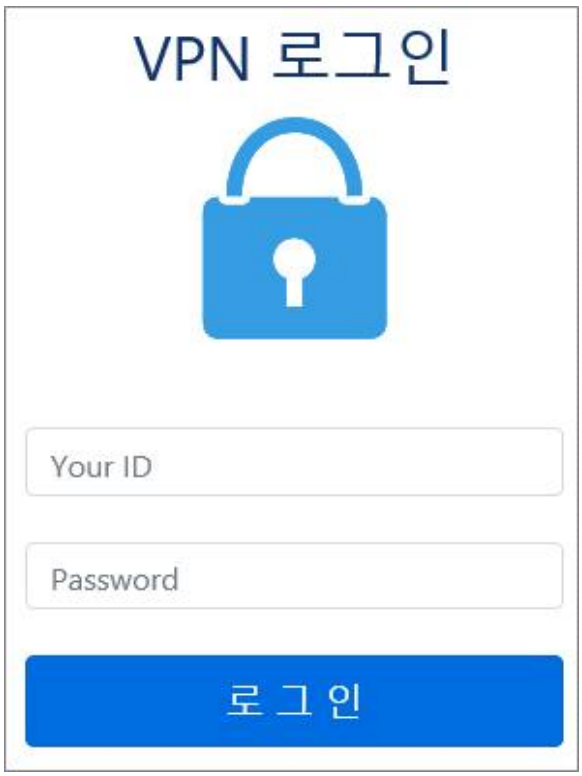
점검 기준

▶ 미조치: 개인정보처리시스템 접속권한을 IP주소 등으로 제한하지 않은 경우
▶ 해당없음: 없음

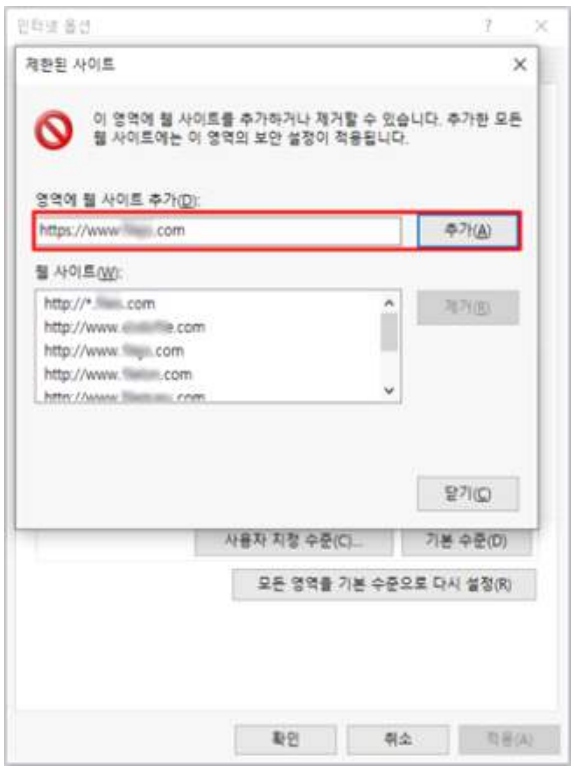
참고 자료

• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p211~212
• 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p52~53

12	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 유출시도를 탐지 및 대응하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제6조(접근통제)** **▶ 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하고 있는지 여부** 1. 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출시도 탐지 및 대응 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	· 침입차단시스템, 침입탐지시스템, 침입방지시스템 등 설치·운영 · 웹방화벽, 보안 운영체제(Secure OS) 등 도입 · 스위치 등의 네트워크 장비에서 제공하는 ACL(Access Control List : 접근제어목록) 등 기능을 이용하여 IP주소 등을 제한함으로써 침입차단 기능을 구현 · 공개용 소프트웨어를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당 기능을 포함한 시스템을 설치·운영 (다만, 공개용 소프트웨어를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검하고 정기적인 업데이트 여부 등 확인 후 적용 필요) · 이외에도, 인터넷데이터센터(IDC), 클라우드 서비스, 보안업체 등에서 제공하는 보안서비스 등도 활용 가능 <침입차단시스템 예시> 
점검 기준	▶ 미조치: 개인정보처리시스템에 접속한 IP주소 등을 불법적인 개인정보 유출시도 미대응 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p211 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p52~53

13	외부에서 개인정보처리시스템에 접속 시, 가상사설망(VPN), 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제6조(접근통제)** **▶ 외부에서 정보통신망을 통한 접속 시 가상사설망(VPN), 전용선 등 안전한 접속수단이나 안전한 인증수단 제공 여부** ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 외부에서 접근가능한 개인정보처리시스템 확인** 1) 외부에서 내부로 접근 가능한 개인정보처리시스템을 확인하고 어떠한 방법(일반적인 접근, VPN, 전용선)으로 접근 가능한지 확인 2) 일반적인 URL 혹은 특정 PORT를 통해 접근 가능 지점이 확인될 경우 반드시 업무상 필요로 하는 지점이 아닌 경우 외부에서 해당 개인정보처리시스템으로의 접근을 통제 3) 반드시 업무상 외부에서의 접근이 필요로 하는 지점일 경우 VPN, 전용선 등 전송구간에 대한 침해사고를 방지할 수 있는 기술적 보안조치 적용 권장 ※ 외부에서 개인정보처리시스템에 접근: 출장, 재택근무 등 기관 외 장소에서 개인정보처리시스템에 접근하는 경우 ※ 가상사설망(VPN : Virtual Private Network) : 개인정보취급자가 사업장 내의 개인정보처리시스템에 대해 원격으로 접속할 때 IPsec이나 SSL 기반의 암호 프로토콜을 사용한 터널링 기술을 통해 안전한 암호통신을 할 수 있도록 해주는 보안 시스템을 의미 ※ 전용선 : 물리적으로 독립된 회선으로서 두 지점 간에 독점적으로 사용하는 회선으로 개인정보처리자와 개인정보취급자, 또는 본점과 지점 간 직통으로 연결하는 회선 등을 의미 <안전한 접속수단 예시> 

점검 방법 및 예시	**2. 안전한 인증수단 제공 여부 확인** 1) 외부에서 내부로 접근할 경우 ID/비밀번호 입력 외에 추가로 PKI, 휴대폰 인증 등 추가 인증수단을 통해 접속하는지 여부 확인 ※ 인증서(PKI, Public Key Infrastructure) : 전자상거래 등에서 상대방과의 신원확인, 거래 사실 증명, 문서의 위·변조 여부 검증 등을 위해 사용하는 전자서명으로서 공인인증서 등 해당 전자서명을 생성한 자의 신원을 확인하는 수단 ※ 보안토큰 : 암호 연산장치 등으로 내부에 저장된 정보가 외부로 복사, 재생성되지 않도록 공인인증서 등을 안전하게 보호할 수 있는 수단으로 스마트 카드, USB 토큰 등이 해당 ※ 일회용 비밀번호(OTP, One Time Password) : 무작위로 생성되는 난수를 일회용 비밀번호로 한번 생성하고, 그 인증값이 한 번만 사용가능하도록 하는 방식 <안전한 인증수단 예시> 
점검 기준	▶ 미조치: 외부에서 개인정보처리시스템 접속 시 안전한 접속수단 및 인증수단 미적용 시 ▶ 해당없음: 개인정보처리시스템 미보유하거나 외부에서 접속이 불가한 경우
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p211 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p52~53

14	개인정보가 인터넷 홈페이지, P2P, 공유설정 등으로 유.노출되지 않도록 개인정보처리시스템, 업무용컴퓨터 등에 접근통제 등에 관한 조치를 하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제6조(접근통제)** **▶ 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 취하고 있는지 확인**
점검 방법 및 예시	**1. P2P, 웹하드, 공유설정 등 사용가능 확인** 1) 내부의 개인정보를 처리하는 단말 혹은 시스템에서 P2P 및 웹하드 등 외부로의 자료 공유가 가능한 지점을 확인합니다. 2) 망분리를 하지 않은 경우 모든 P2P와 웹하드에 대해 통제를 하기 어려우나 잘 알려진 공유 프로그램에 대해서는 반드시 보안장비의 허용거부 등의 정책 적용이 필요합니다. 3) P2P, 공유설정이 업무상 꼭 필요한 경우라도 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여야 합니다. <윈도우 파일 공유 설정 예시>  [폴더] – [속성] – [공유] – [공유] - 소유자 이외의 계정 [제거] <윈도우 제한된 사이트 설정 예시>  [인터넷] - [설정] - [인터넷 옵션] - [보안] - [제한된 사이트] - [사이트] - [영역에 웹 사이트 추가] - P2P사이트[추가]

점검 방법 및 예시

2. 공개된 무선망을 이용하여 개인정보 처리하는 경우 유출 차단 조치 확인

1) 고유식별정보 송·수신 시 SSL, VPN 등이 적용된 전용 프로그램을 사용하는지 확인합니다.
2) 고유식별정보가 포함된 파일 송·수신 시 파일 암호화 저장 후 송·수신하는지 확인합니다.
3) 공개된 무선망 이용 시, 무선접속장치(AP)에 안전한 비밀번호가 적용된 WPA2(Wi-Fi Protected Access 2) 보안 프로토콜을 사용하는지 확인합니다.

<SSL 인증서>

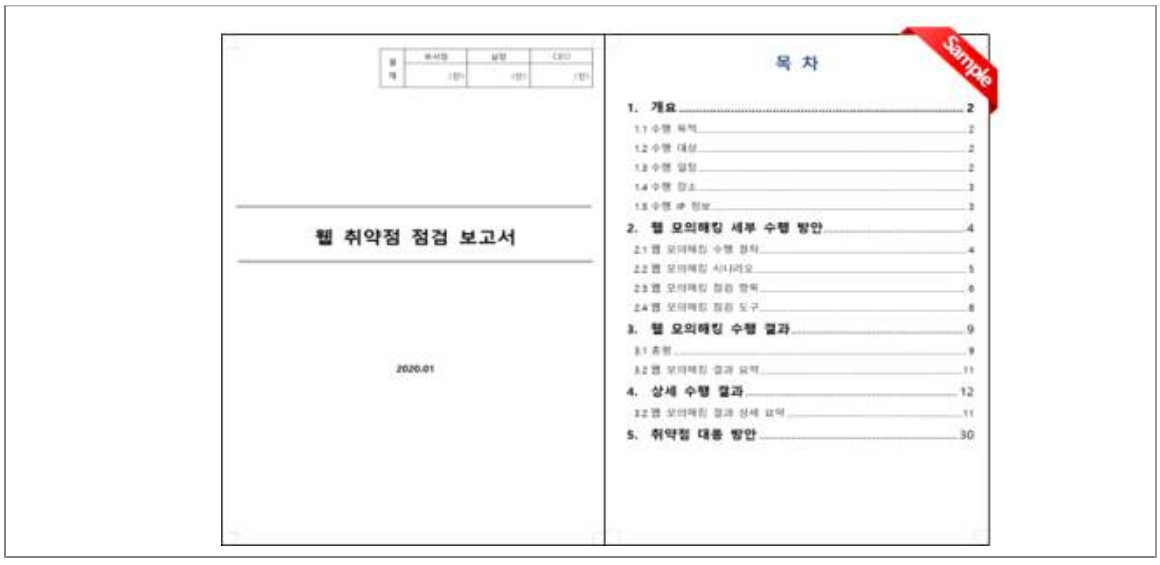
<무선접속장치 WPA2 보안>

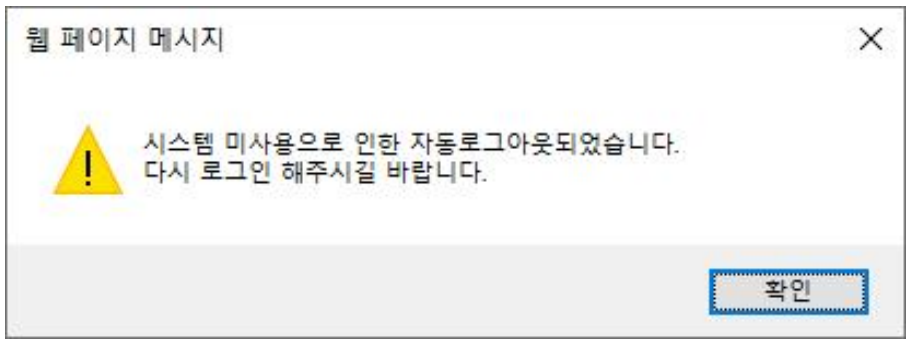
점검 기준

▶ 미조치: P2P, 공유설정의 사용에 대하여 접근통제 미적용 시
▶ 해당없음: 없음

참고 자료

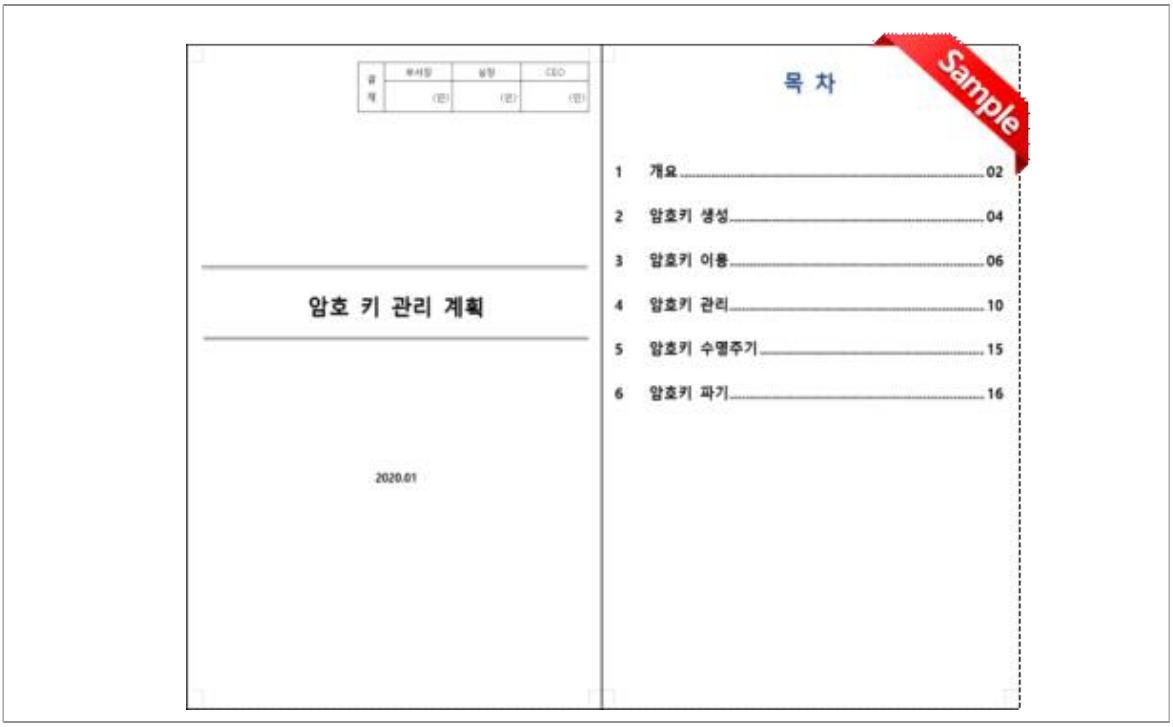
- 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p211~212
- 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p55~55

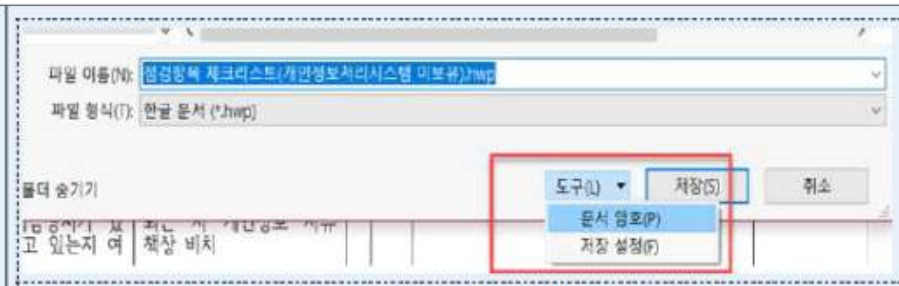
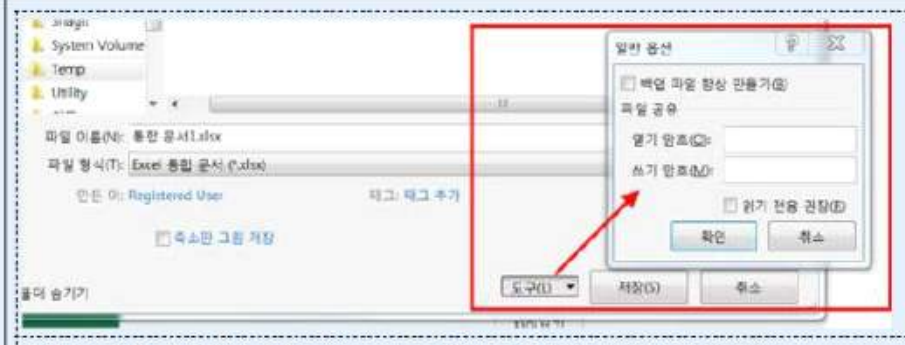
15	인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우, 해당 홈페이지에 대해 연 1회 이상 취약점을 점검 및 그에 따른 개선조치를 하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제6조(접근통제)** ▶ **인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하는지 여부 확인** ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 시큐어 코딩을 적용한 개발 방안 마련하였는지 여부 확인** 1) 각종 보안 가이드라인을 참고하여 시큐어 코딩을 하였는지 여부를 확인합니다. <시큐어 코딩 참고자료> - 공개소프트웨어를 활용한 소프트웨어 개발보안 점검가이드 (행정안전부, 2019.06.) - 소프트웨어 보안약점 진단가이드 (행정안전부, 2019.06.) - 소프트웨어 개발보안 가이드 (행정안전부, 2019.11.) - 시큐어코딩가이드(C, JAVA) (행정안전부, 2012.09.) - Web 2.0 정보보호 실무가이드 (행정안전부, 2010.05.) - 홈페이지 취약점 진단·제거 가이드 (KISA, 2013.12.) 등 **2. 고유식별정보 처리 시, 연 1회 이상 취약점 점검 실시 여부 확인** 1) 연 1회 이상 인터넷 홈페이지에 대한 취약점 점검을 실시하였는지 확인합니다. ※ 취약점 점검 시 개인정보처리자의 자체인력, 보안업체 등을 활용할 수 있으며, 취약점 점검은 상용 도구, 공개용 도구, 자체 제작 도구 등을 사용 <웹 취약점 점검 보고서 예시> 
점검 기준	▶ 미조치: 인터넷 홈페이지에 대하여 연 1회 이상 취약점 점검 미실시 시 ▶ 해당없음: 인터넷 홈페이지를 통해 고유식별정보를 처리하지 않는 경우
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p211~212 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p52~53

16	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 개인정보처리시스템에 접속을 차단하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제6조(접근통제)** ▶ **개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 개인정보처리시스템에 접속을 차단하고 있는지 여부** ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 일정시간 이상 업무처리를 하지 않을 경우, 자동으로 시스템 접속차단 여부 확인** 1) 일정시간 개인정보처리시스템 미사용 시 계정에 대한 접속차단이 이루어지는지 확인합니다. 2) 시스템 재접속 시 최초의 로그인과 동일한 방법으로 접속하는지 확인합니다. <세션 타임아웃 설정 예시>  <세션 타임아웃 설정에 따른 팝업 예시> 
점검 기준	▶ 미조치: 일정시간 이상 업무처리를 하지 않을 경우, 개인정보처리시스템에 대한 접속 미차단 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p205 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p58

17	고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)** **▶ 고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는지 여부**
점검 방법 및 예시	**1. 정보통신망을 통하여 송·수신하는 고유식별정보를 확인합니다.** 1) SSL 적용 또는 안전한 암호화 알고리즘을 사용하여 송·수신하는 고유식별정보를 암호화하는지 확인합니다. <SSL 인증서 예시>  **2. 보조저장매체를 통하여 전달하는 고유식별정보를 확인합니다.** 1) 암호화 기능을 제공하는 보안 USB 등의 보조저장매체를 사용하는지 확인합니다. 2) 해당 개인정보를 암호화하여 보조저장매체를 사용하는지 확인합니다. <보안 USB> 
점검 기준	▶ 미조치: 고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우, 암호화 미조치 시 ▶ 해당없음: 고유식별정보를 송신 또는 보조저장매체를 통해 전달하지 않는 경우
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p212~213 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p61~70 • 행정안전부, 한국인터넷진흥원, "개인정보의 암호화 조치 안내서(2017.1.)"

18	내부망에 고유식별정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)** **▶ 내부망에 고유식별정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는지 여부** ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 내부망에 고유식별정보 저장 여부 확인** 1) 내부망에 저장 중인 고유식별정보가 있는지 확인합니다. 2) 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있습니다. 1.「개인정보 보호법」제33조 및 시행령 제35조에 따라 영향평가의 대상이 되는 개인정보파일을 운용하는 공공기관은 해당 "개인정보 영향평가"의 결과 2. 공공기관 이외의 개인정보처리자는 암호화 미적용 시 "위험도 분석"에 따른 결과 ※ "개인정보 영향평가 수행 안내서" 및 "개인정보 위험도 분석 기준 및 해설서"는 개인정보보호 종합포털(http://www.privacy.go.kr)에서 다운로드 가능 ※ 안전한 암호알고리즘, 암호화 방식 등은 "개인정보의 암호화 조치 안내서"를 참조하고, 해당 자료는 개인정보보호 종합포털(http://www.privacy.go.kr)에서 다운로드 가능 다만, 내부망에 주민등록번호를 저장하는 경우, 개인정보 보호법 제24조의2, 동법 시행령 제21조의2에 따라 "개인정보 영향평가"나 암호화 미적용 시 "위험도 분석"의 결과와 관계없이 암호화하여야 합니다. **2. 고유식별정보 전송 및 보관 시 암호화 여부 확인** 1) 내부망에 고유식별정보를 안전한 암호화 알고리즘을 사용하여 암호화를 하고 있는지 확인합니다. 2) 암호화 미조치 중일 경우에는, 영향평가나 위험도분석 결과를 따른 것인지 확인하여 점검결과에 반영합니다. <고유식별정보 암호화 예시> USER_ID | USER_NAME | USER_PASSPORT gdhong1 | 홍길동 | 4D49CA0443BE87F6EFF65F63508FF8F27954EAA051DF0FE1BAA318179439B60C koreak | 김한국 | 502A6EB322C7D88340AAB36BF946EF37D7735E73ED339F9BACBD7182BACB5D3 information | 박정보 | 14272360DF010A49218539DD8F8C08189427477AE8EB4B50B071A42E386C35E5 ※ 영향평가 결과 또는 위험도분석 결과에 따른 암호화 미조치의 경우 자체점검 결과는 "조치"로 표시 ※ 100만 명 이상의 주민등록번호를 보관하는 개인정보처리자가 암호화 미조치 중일 경우, 영향평가 결과 또는 위험도분석 결과에 따른 것이면 "조치", 그렇지않은 경우에는 "미조치"로 표시
점검 기준	▶ 미조치: 내부망에 고유식별정보를 저장하는 경우, 암호화 미조치 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p212~213 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p61~70 • 행정안전부, 한국인터넷진흥원, "개인정보의 암호화 조치 안내서(2017.1.)"

19	암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)** ▶ **암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립 여부** ※ 개인정보처리시스템 미보유 시 점검하지 않음 ※ 유형2일 시 점검하지 않음
점검 방법 및 예시	**1. 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립・시행 여부 확인** 1) 암호키와 관련된 절차를 수립하여 시행하고 있는지 확인합니다. 2) 개인정보의 암호화 조치 안내서를 참조합니다. <암호키 관리 계획 예시> 
점검 기준	▶ 미조치: 암호키를 안전하게 보관하기 위한 절차 미수립 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p212~213 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p61~70 • 행정안전부, 한국인터넷진흥원, "개인정보의 암호화 조치 안내서(2017.1.)" • 과학기술정보통신부, 한국인터넷진흥원, "암호키 관리 안내서(2014.12.)"

20	업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)** **▶ 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우, 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하는지 여부**
점검 방법 및 예시	**1. 업무용 컴퓨터 또는 모바일 기기 등에 고유식별정보를 포함한 파일이 있는지 확인** 1) 개인정보처리시스템 또는 업무용 컴퓨터 내에 고유식별정보를 포함한 데이터베이스, 파일 등이 있는지 확인합니다. **2. 암호화 여부 확인** 1) 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하였는지 확인합니다. <고유식별정보 암호화 예시> USER_ID / USER_NAME / USER_PASSPORT gdhong1 / 홍길동 / 4D49CA0443BE87F6EFF65F63508FF8F27954EAA051DF0FE1BAA318179439B60C koreak / 김한국 / 502A6EB322C7D88340AAB36BF946EF37D7735E73ED339F9BACBD7182BACB5D3 information / 박정보 / 14272360DF010A49218539DD8F8C08189427477AE8EB4B50B071A42E386C35E5 <문서파일 암호화 예시> 한컴 오피스 (hwp)  파일 》 다른 이름으로 저장하기 》 문서 암호 설정에서 암호 설정 가능 MS 오피스 (Excel)  파일 》 다른 이름으로 저장하기 》 도구 》 일반옵션에서 암호 설정 가능
점검 기준	▶ 미조치: 업무용 컴퓨터, 모바일 기기에 저장된 고유식별정보 암호화 미조치 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p212~213 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p61~70 • 행정안전부, 한국인터넷진흥원, "개인정보의 암호화 조치 안내서(2017.1.)"

21	개인정보취급자가 개인정보처리시스템에 접속한 기록을 2년 이상 보관·관리하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)** **▶ 개인정보처리시스템에 접속한 기록을 2년 이상 보관·관리하고 있는지 여부** ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	**1. 개인정보처리시스템 내 접속기록 로그 확인** 1) 개인정보처리시스템 내 접속기록 로그를 확인합니다. 2) 접속기록 로그를 2년 이상 관리하고 있는지 확인합니다. <접속기록 로그 확인 예시>
점검 기준	▶ 미조치: 개인정보처리시스템에 접속한 기록을 2년 이상 보관, 관리하고 있지 않은 경우 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p214 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p71~74

개인정보 로그조회 발생일자 2017-12-01 ~ 2020-02-28 A1101 조회

번호	로그ID	접속시간	IP	처리정보	수행업무	상세보기
1	kim112	2017.12.01 13:00:03	192.168.1.40	A1101	등록	
2	kim112	2017.12.01 13:01:28	192.168.1.40	A1101	수정	
3	han122	2018.01.14 09:38:08	192.168.1.30	A1101	조회	
4	joo890	2018.02.01 10:00:00	192.168.1.60	A1101	조회	
5	joo890	2018.02.01 10:01:12	192.168.1.60	A1101	수정	
6	han122	2019.12.16 12:03:01	192.168.1.30	A1101	조회	
7	kim112	2020.02.09 14:54:09	192.168.1.40	A1101	삭제	

22 개인정보취급자가 개인정보처리시스템에 접속한 기록에는 사용자 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행한 업무내용 등이 포함되어 있는지 여부

관련 규정

개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)

▶ **개인정보처리시스템에 접속한 기록에 필수사항 5가지가 모두 포함되어 있는지 여부**

※ 개인정보처리시스템 미보유 시 점검하지 않음

- **계정** : 개인정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID 등 계정정보
- **접속일시** : 접속한 시간 또는 업무를 수행한 시간(년-월-일, 시:분:초)
- **접속지 정보** : 개인정보처리시스템에 저속한 자의 컴퓨터 또는 서버의 IP주소 등
- **처리한 정보주체 정보** : 개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 식별정보 (ID, 고객번호, 학번, 사번 등)
  ※ 기록하는 정보주체 정보의 경우 민감하거나 과도한 개인정보가 저장되지 않도록 하여야 함
- **수행업무** : 개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용을 알 수 있는 정보
  ※ 개인정보에 대한 수집, 생성, 연계, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 등이 수행업무에 해당될 수 있다.

점검 방법 및 예시

1. 개인정보처리시스템 내 접속기록 로그 확인

1) 개인정보처리시스템 내 접속기록 로그를 확인합니다.

2) 접속기록 로그에 5가지 필수사항이 모두 포함되어 있는지 확인합니다.

<접속기록 항목 예시>

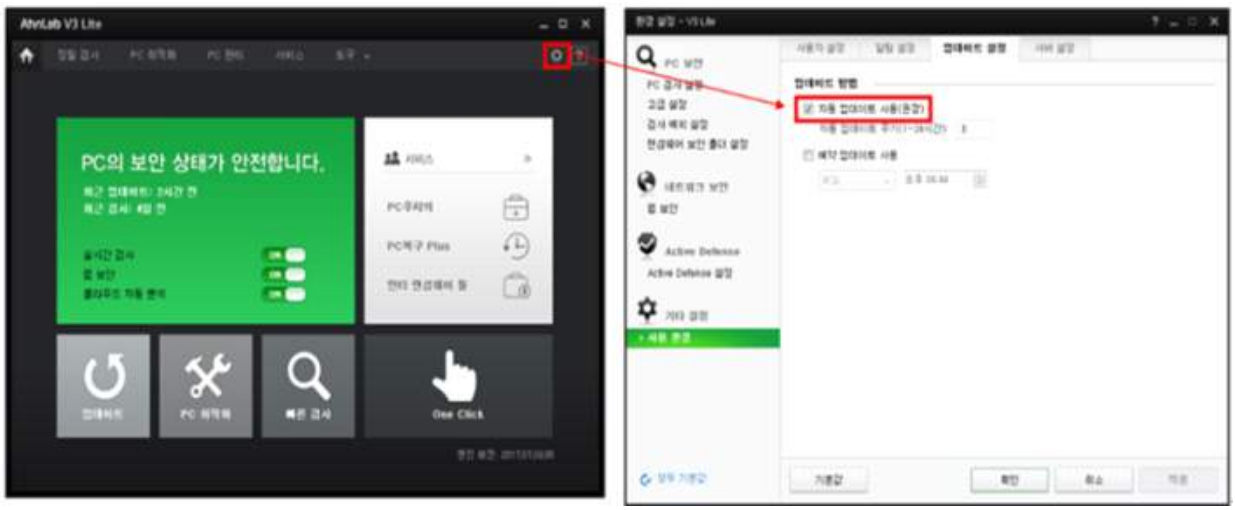
점검 기준

▶ 미조치: 개인정보처리시스템에 접속한 기록에 5가지 필수 항목 누락 시

▶ 해당없음: 없음

참고 자료

- 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p214
- 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p71~74

23	악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치·운영 및 최신의 상태로 유지하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제9조(악성프로그램 등 방지)** **▶ 악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치·운영하고 최신의 상태로 유지하고 있는지 여부** 1. 보안프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지 2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시 3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치
점검 방법 및 예시	**1. 백신 소프트웨어 설치·운영** 1) 단말기 내 보안프로그램 설치 여부를 확인합니다. 2) 보안프로그램이 항상 실행되어 있는지 여부를 확인합니다. **2. 백신 소프트웨어 최신 업데이트** 1) 일 1회 이상 업데이트를 실시하는지 여부를 확인합니다. 2) 보안프로그램 제작업체의 보안 업데이트 공지가 있는지 확인합니다. <백신프로그램 설치 및 업데이트 예시> 

점검 방법 및 예시

3. 발견된 악성프로그램에 대한 대응 조치

1) 보안프로그램을 통해 발견된 악성프로그램 등에 대하여 삭제, 치료 등의 대응조치를 하는지 확인합니다.

2) 발견된 악성프로그램에 대하여 삭제, 치료가 어려운 경우에는 개인정보처리시스템, 업무용 컴퓨터 등을 분리하는 등의 악성프로그램 확산 방지를 위한 적절한 안전조치를 취하는지 확인합니다.

<KISA 선정 PC용 우수 백신프로그램 10종>

프로그램명	업체명
내주치의 닥터	KT
네이버 백신	NHN
바이로봇 Internet Security 2011	하우리
알약	이스트소프트
터보백신 라이트	에브리존
터보백신 인터넷 시큐리티	
nProtect AVS 3.0	잉카인터넷
TC스파이닥터	프리아이커뮤니케이션
V3 365 클리닉	안랩
V3 Lite	

점검 기준

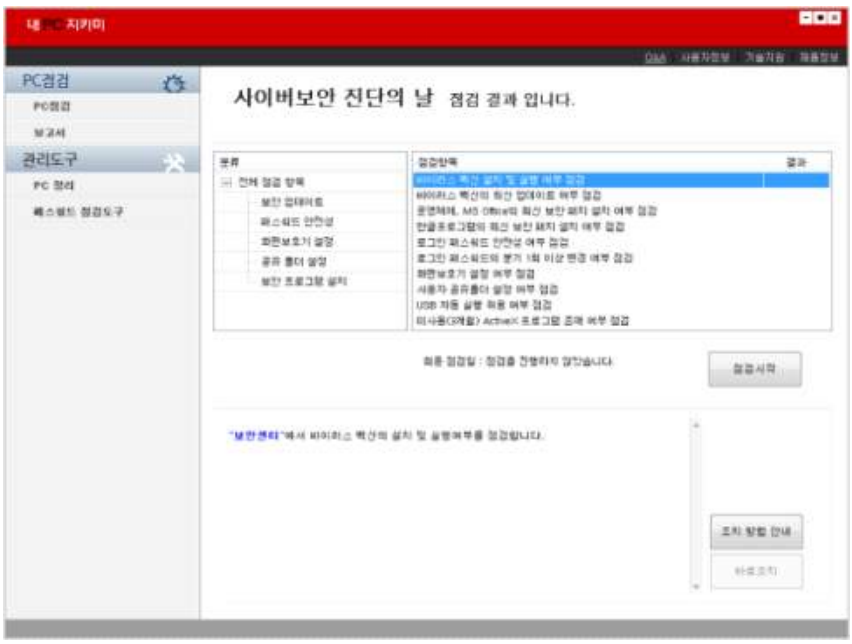
▶ 미조치: 백신프로그램을 설치하지 않거나, 일 1회 이상 업데이트 미설정 시

▶ 해당없음: 없음

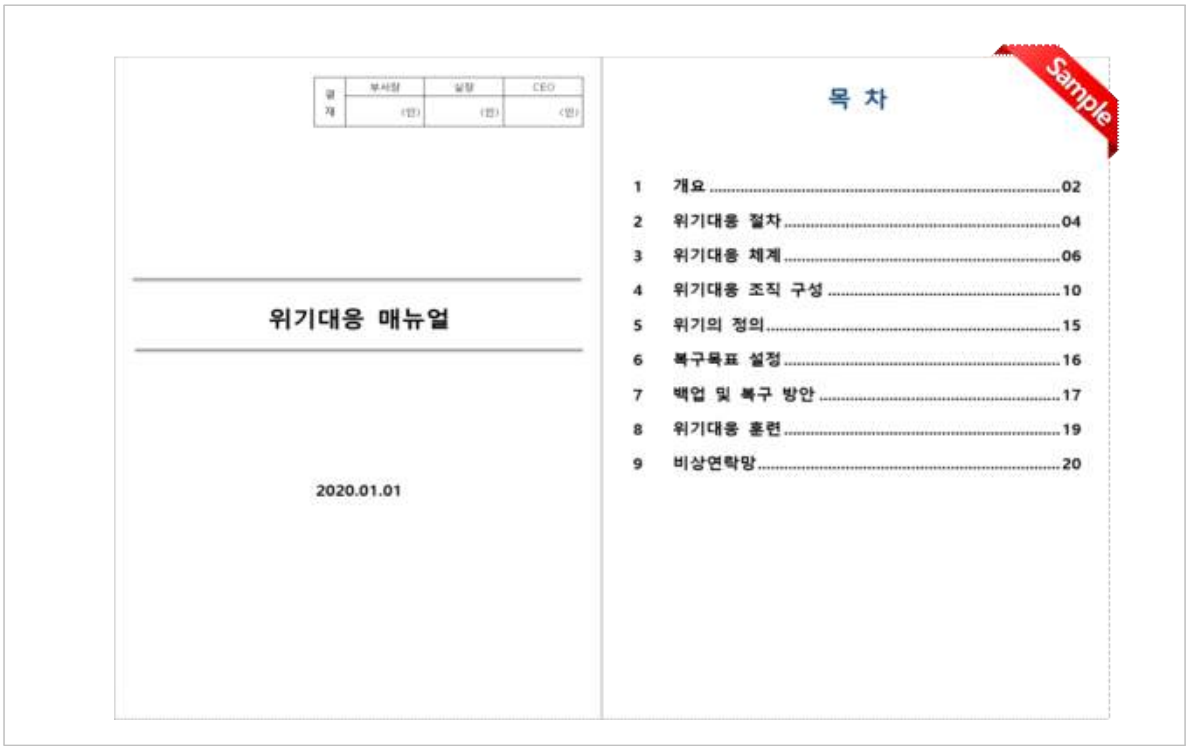
참고 자료

• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p214

• 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p75~76

24	개인정보처리시스템에 직접 접속하는 관리용 단말기에 대해 비인가자가 임의로 조작하지 못하도록 조치하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제10조(관리용 단말기의 안전조치)** **▶ 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대하여 안전조치를 하는지 여부** 1. 인가받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 2. 본래 목적 외로 사용되지 않도록 조치 3. 악성프로그램 감염 방지 등을 위한 보안조치 적용 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법 및 예시	· 관리용 단말기 현황 관리(IP주소, 용도, 담당자, 설치 위치 등) ※ 관리용 단말기: 개인정보처리시스템에 대하여 직접 접속하여 해당 시스템을 개발·운영·관리하는 기기 · 중요 관리용 단말기를 지정하여 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 · 관리용 단말기에 주요 정보 보관 및 공유 금지 · 비인가자 접근을 방지하기 위한 부팅암호, 로그인 암호, 화면보호기 암호 설정 · 보조기억매체 및 휴대용 전산장비 등에 대한 접근통제 · 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지 등 · 악성코드 감염 방지를 위한 보안프로그램의 최신상태 유지, 보안 업데이트 적용, 악성프로그램 삭제 등 대응 조치 · 보안 상태 및 사용현황에 대한 정기 점검 등 <관리용 단말기 안전조치 예시> 
점검 기준	▶ 미조치: 관리용 단말기에 대해 안전조치를 하지 않을 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p214 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p71~74

25	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 장소에 보관하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제11조(물리적 안전조치)** **▶ 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있는지 확인** 1. 개인정보가 포함된 서류, 보조저장매체(이동형 하드디스크, USB메모리, SSD 등) 등은 금고, 잠금장치가 있는 캐비넷 등 안전한 장소에 보관
점검 방법 및 예시	**1. 개인정보의 안전한 보관 여부 확인** 1) 개인정보가 포함된 서류, 보조저장매체 등이 시건장치, 자물쇠 등 잠금장치가 있는 캐비넷, 전산실, 자료보관실 등에 보관되고 있는지 여부를 확인합니다. <시건장치가 있는 캐비넷>  <출입통제시스템> 
점검 기준	▶ 미조치: 개인정보가 포함된 서류, 보조저장매체 등에 대하여 물리적 안전조치를 하지 않을 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p215 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p79~80

26	재해·재난 발생 시, 개인정보의 손실·훼손 등을 방지하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제12조(재해·재난 대비 안전조치)** **▶ 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 있는지 확인** 1. 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 문서화하여 이에 따라 대처 2. 대응절차의 적정성과 실효성을 보장하기 위하여 정기적으로 점검 ※ 개인정보처리시스템 미보유 시 점검하지 않음 ※ 유형2일 시 점검하지 않음
점검 방법 및 예시	**1. 위기대응 매뉴얼 등 재해·재난 시 절차 수립 여부 확인** 1) 재해·재난 시 개인정보의 손실 및 훼손 등을 방지하기 위한 위기대응 매뉴얼 수립 여부를 확인합니다. <위기대응 매뉴얼 예시>  **2. 위기대응 절차 정기적 점검** 1) 수립된 대응절차에 대하여 정기적으로 점검하여 대응절차에 변경이 있는 경우 변경사항을 반영하는 등의 적절한 조치를 취해야 합니다.
점검 기준	▶ 미조치: 재해·재난 발생 시, 위기대응 매뉴얼 등 대응절차를 마련하지 않을 시 ▶ 해당없음: 없음
참고 자료	• 행정안전부, "개인정보보호 법령 및 지침·고시 해설(2016.12.)", p215 • 행정안전부, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2019.6.)", p81~83

7 기관현황 및 점검결과 수정

(개인정보보호 종합포털 → 고유식별정보 실태조사 안내(기관현황/자체점검) → 본인인증)
본인인증이 완료되면, 등록된 기관현황 정보 및 자체점검 결과를 수정 가능합니다.

※ 수정 가능기간 : 등록이후 ~ 제출일('20.8.31.)전 까지

점검결과

조치 (있음)	미조치 (없음)	해당 없음
18	6	0

● 고유식별정보 안전조치 자체점검

번호	세부 점검내용	점검결과	설명
1	주민등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거가 있는지 여부	조치	
2	여권번호, 운전면허번호, 외국인등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거 또는 정보주체의 동의가 있는지 여부	조치	
3	수집목적이 달성되었고, 보존기간이 경과한 고유식별정보를 파기하고 있는지 여부	조치	
4	개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행하고 있는지 여부	조치	
5	개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는지 여부	조치	
6	전보 또는 퇴직 등 개인정보취급자 변경 시, 개인정보처리시스템에 대한 접근권한을 변경 또는 말소하고 있는지 여부	조치	
7	개인정보처리시스템에 대한 개인정보취급자의 접근권한 부여·변경·말소 내역을 기록하고 있으며 3년간 보관하고 있는지 여부	조치	
8	개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지 않는지 여부	조치	
9	개인정보취급자 또는 정보주체가 안전한 비밀번호 작성규칙을 수립하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하고 있는지 여부	조치	
10	사용자계정 또는 비밀번호를 일정 횟수이상 잘못 입력한 경우, 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는지 여부	조치	
11	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하고 있는지 여부	조치	
12	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 유출시도를 탐지 및 대응하고 있는지 여부	조치	
13	외부에서 개인정보처리시스템에 접속 시, 가상사설망(VPN), 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하고 있는지 여부	조치	
14	개인정보가 인터넷 홈페이지, P2P, 공유설정 등으로 유노출되지 않도록 개인정보처리시스템, 업무용컴퓨터 등에 접근통제 등에 관한 조치를 하고 있는지 여부	조치	
15	인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우, 해당 홈페이지에 대해 연 1회 이상 취약점을 점검 및 그에 따른 개선조치를 하고 있는지 여부	조치	
16	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 개인정보처리시스템에 접속을 차단하고 있는지 여부	조치	
17	고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는지 여부	조치	
18	내부망에 고유식별정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는지 여부	조치	
19	암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립 여부	-	
20	업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하는지 여부	미조치	
21	개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하고 있는지 여부	미조치	
22	개인정보취급자가 개인정보처리시스템에 접속한 기록에는 사용자 계정, 접속일시, 접속지 정보, 수행한 업무내용 등이 포함되어 있는지 여부	미조치	
23	악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영 및 최신의 상태로 유지하고 있는지 여부	미조치	
24	개인정보처리시스템에 직접 접속하는 관리용 단말기에 대해 비인가자가 임의로 조작하지 못하도록 조치하고 있는지 여부	미조치	
25	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 장소에 보관하고 있는지 여부	미조치	
26	재해·재난 발생 시, 개인정보의 손실·훼손 등을 방지하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 있는지 여부	-	

※ 해당 점검항목별 대상기관 전체의 안전성 확보조치 이행결과를 입력

※ 고유식별정보가 포함된 개인정보처리시스템을 한개 이상 보유하고 있는 기관의 경우, 관련점검 항목에서 "조치"로 입력하기 위해서는 모든 처리시스템에서 해당 조치를 완료하여야 함 (1개의 처리시스템이라도 안되었을 경우에는 "미조치"로 입력)

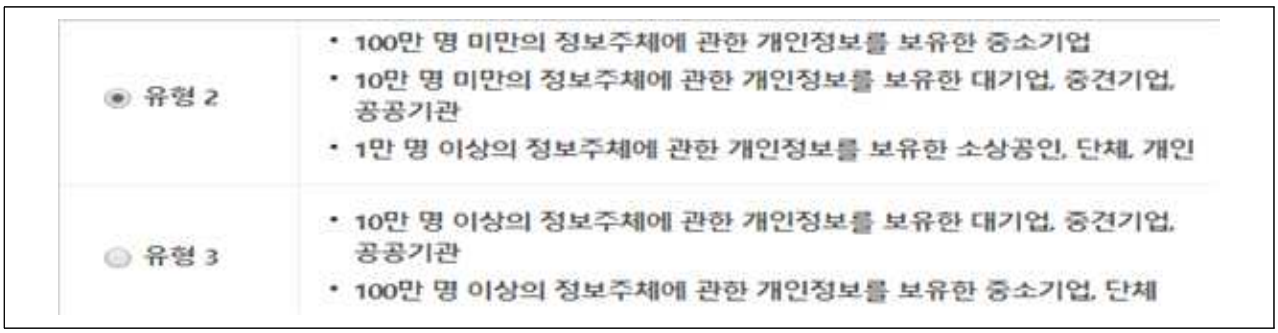
※ 상기 점검항목에서의 개인정보처리시스템은 고유식별정보가 포함된 개인정보처리시스템을 말함

※ 1926번 항목은 유형3만 해당

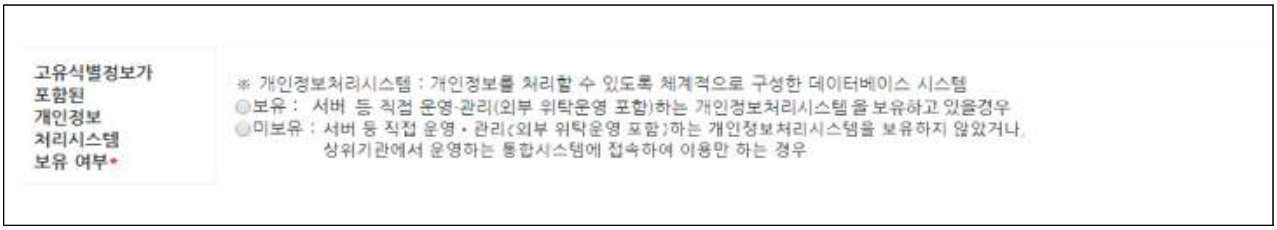
다운로드 인쇄 수정

※ 기관 유형 변경, 개인정보처리시스템 보유/미보유 변경시 주의사항

다음의 경우에는 고유식별정보 안전조치 자체점검을 다시 작성하여야 합니다.



[그림 1] 유형을 변경하는 경우



[그림 2] 개인정보처리시스템 보유여부를 변경하는 경우

- '유형' 또는 '보유/미보유' 변경 후 자체점검 작성 중에 저장하지 않고 웹 브라우저를 닫은 경우에는 재접속하신 후 자체점검 수정버튼을 눌러서 다시 작성해주세요

8 개인정보의 안전성 확보조치 기준

개인정보의 안전성 확보조치 기준

[시행 2019. 6. 7.] [행정안전부고시 제2019-47호]

행정안전부(개인정보보호정책과) 04-205-2842

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제23조제2항, 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. "대기업"이란 「독점규제 및 공정거래에 관한 법률」 제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
5. "중견기업"이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조에 해당하는 기업을 말한다.
6. "중소기업"이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.
7. "소상공인"이란 「소상공인 보호 및 지원에 관한 법률」 제2조에 해당하는 자를 말한다.
8. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
9. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
10. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
11. "위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
12. "비밀번호"란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
13. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
14. "공개된 무선망"이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한

다.

15. "모바일 기기"란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
16. "바이오정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
17. "보조저장매체"란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
18. "내부망"이란 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
19. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
20. "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(안전조치 기준 적용) 개인정보처리자가 개인정보의 안전성 확보에 필요한 조치를 하는 경우에는 [별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준을 적용하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대한 입증책임은 당해 개인정보처리자가 부담한다.

제4조(내부 관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항
4. 접근권한의 관리에 관한 사항
5. 접근통제에 관한 사항
6. 개인정보의 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항
8. 악성프로그램 등 방지에 관한 사항
9. 물리적 안전조치에 관한 사항
10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
11.개인정보 유출사고 대응 계획 수립·시행에 관한 사항
12. 위험도 분석 및 대응방안 마련에 관한 사항
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 그 밖에 개인정보 보호를 위하여 필요한 사항

② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지

아니할 수 있다.
③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.
④ 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검·관리 하여야 한다.

제5조(접근권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.
② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.
③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.
⑥개인정보처리자는 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.
⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.

제6조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.
1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP (Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.
③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 한다.
④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.
⑤개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.
⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제9조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제10조(관리용 단말기의 안전조치) 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

제11조(물리적 안전조치) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제12조(재해·재난 대비 안전조치) ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.

제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

부칙 <제2017-1호, 2017. 7. 26.>

제1조(시행일) 이 고시는 발령한 날부터 시행한다.

부칙 <제2019-47호, 2019. 6. 7.>

제1조(시행일) 이 고시는 고시한 날부터 시행한다.

제2조(재검토기한) 행정안전부장관은 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2019년 7월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 6월 30일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.