2021년 고유식별정보 안전조치 관리실태 조사 매뉴얼(민간)

2021년 4월



개인정보보호위원회



한국인터넷진흥원

목 차

1. 조사개요 ····· 3

2. 참고 및 유의사항 ····· 5

3. FAQ ····· 7

4. 시스템 사용 방법 ····· 11

4-1. 담당자 등록 방법 ····· 11

4-2. 기관현황 등록 방법 ····· 13

4-3. 자체점검 제출 방법 ····· 18

4-4. 증빙자료 제출 방법 ····· 19

4-5. 수정 방법 ····· 21

5. 점검방법 ····· 26

5-1. 자체점검 점검항목 ····· 26

5-2. 증빙자료 제출 점검항목 ····· 28

5-3. 점검항목 세부안내 ····· 29

1 조사개요

1. 목적

o 공공기관 및 5만 명 이상의 고유식별정보처리자 대상, 정기조사를 통해 안전조치 이행현황을 점검·지원

o 고유식별정보처리자의 안전성 확보조치 의무에 대한 경각심을 지속적으로 유지하고, 침해사고에 대한 사전예방 등 선제적 대응체계 마련

2. 조사내용

	공공분야	민간분야
조사대상	초·중등교육법에 따른 각 급 학교	**5만 명 이상 정보주체의 고유식별정보를 처리하는 자**
조사주기	2년 1회 이상	
조사항목	고유식별정보(주민등록번호, 운전면허번호, 여권번호, 외국인등록번호) 보유현황	
	고유식별정보에 대한 안전성 확보조치 이행 여부	
조사방법	**1. 개인정보보호 포털을 통해 기관 및 담당자정보, 고유식별정보 보유 현황 등록** **2. 고유식별정보 안전조치 이행현황 자체점검 결과등록** **3. 점검항목 증빙자료 제출** ※ 결과 확인 후 증빙자료 검토 및 개선안내 / 필요시 현장점검	
조사기관	개인정보보호위원회, 한국인터넷진흥원	

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 보호위원회는 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 보호위원회는 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 제30조 또는 제48조의2를 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 보호위원회는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에 대하여 법 제24조제4항에 따라 안전성 확보에 필요한 조치를 하였는지를 2년마다 1회 이상 조사해야 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 보호위원회가 정하여 고시하는 법인, 단체 또는 기관

4. 조사절차

①	대상기관 현황조사 및 시행 안내
②	안전조치 이행결과 · 증빙자료 접수 및 컨설팅
③	증빙자료 검토 및 개선안내
④	현장점검

2 참고 및 유의사항

1. **'21년 민간**분야 관리실태 **조사 대상은 5만명 이상 고유식별정보를 처리하는 모든 사업자**입니다.('20년 보건복지 분야 조사 기관 제외)
   개인정보보호 포털(privacy.go.kr)의 본인인증 과정을 거쳐야 기관현황 등록 및 자체점검을 진행할 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 '21. 7. 30.(금)까지** 입니다.
   제출일 전까지는 점검항목별 조치결과 및 증빙자료에 대한 수정이 가능하오니, 미조치 사항은 해당 기한까지 조치를 완료하여 반영 부탁드립니다.
   ☞ 대상기관은 제출일 전까지 기관현황, 자체점검 등록, 증빙자료 제출을 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**

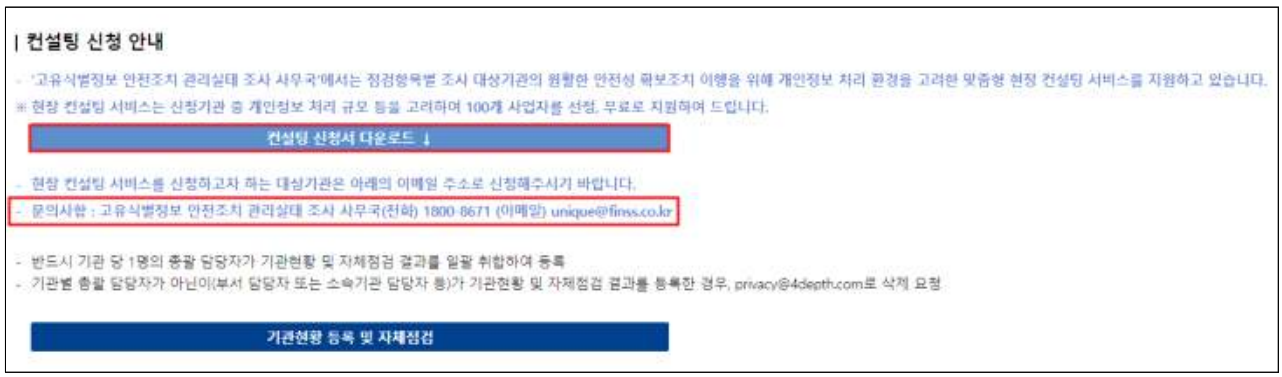
- **고유식별정보 안전조치 관리실태 조사 안내 동영상 등 매뉴얼**
  (개인정보보호 포털 → 지원마당 → 고유식별정보 실태조사 → 자체점검 참고사항)
- 개인정보의 안전성 확보조치 기준 해설서
- 개인정보보호 법령 및 지침·고시 해설서
- 개인정보 암호화 조치 안내서
- 개인정보 위험도 분석 기준 및 해설서
  (개인정보보호 포털 → 자료마당 → 지침자료에서 다운로드 가능)
- 표준 개인정보 보호지침
  (개인정보보호 포털 → 법령자료 → 행정규칙에서 다운로드 가능)

6. 조사 관련 전반적인 사항에 대해 도움이 필요하실 때는 안전조치 무료 현장컨설팅 신청이 가능합니다.

① 개인정보보호 포털 내 지원마당의 고유식별정보 실태조사 페이지 하단의 자체점검 항목을 클릭 후 컨설팅 신청 안내를 확인합니다.



② [신청서다운로드] 버튼을 클릭하여 필요한 자료를 내려받아 신청서를 작성한 뒤, 하단의 고유식별정보 사무국 이메일주소 (unique@finss.co.kr)로 신청서를 보냅니다.



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

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

3 FAQ

Q1	**관리실태 조사 대상기관에 해당하면, 기관현황 및 자체점검 결과만 등록하면 되나요? 그 이후에 추가로 해야 하는 것은 없나요?**

개인정보보호 포털(privacy.go.kr)에 접속하여 고유식별정보 보유현황 등 기관현황에 대한 정보를 등록하고, 안전성 확보조치 이행 여부 확인을 위한 자체점검을 진행하여 결과를 등록하면 됩니다. 대상기관이 기관현황 및 자체점검 결과를 '21. 7. 30.(금)까지 등록완료 하였다면, 추가적으로 조치하여야 할 사항은 없습니다.

Q2	**'21. 7. 30.(금)까지 안전조치 자체점검 결과를 등록하지 않을 경우, 어떠한 처벌을 받게 되나요?**

조사 기간 내 자체점검 결과등록을 하지 않은 것에 대한 직접적인 처벌규정은 없습니다. 다만, 조사 대상기관에 해당하나 결과를 제출하지 않은 미제출기관에 대해서는 개인정보보호 현장점검을 통해 안전조치 미비 사항이 확인될 경우 과태료 등 행정처분이 가중될 수 있습니다.

Q3	**고유식별정보 보유량이 5만 건이 안 되는데 조사대상인가요?**

고유식별정보를 보유하고 있지 않거나 보유하더라도 5만 건이 안 되는 경우, 조사대상이 아닙니다. 본 조사는 내부직원의 고유식별정보도 보유량에 포함하여 진행하고 있습니다. 보유량을 산정할 때는 고유식별정보가 포함된 개인정보처리시스템뿐만 아니라 종이 문서, 업무용 PC에 포함된 고유식별정보도 포함해 주시면 됩니다.

Q4	**법인 합산 시 고유식별정보 보유량이 5만 건이 넘으나 법인별로 5만 건이 되지 않는 경우, 조사를 이행하지 않아도 되나요?**

계열사가 아닌 통합 관리하는 그룹이 조사대상에 해당합니다.

Q5	**법인 내에 관리체계가 완전히 다른 독립된 사업부가 2개인 경우, 등록 시 법인명(사업부명)으로 등록하고 자체점검 진행하면 되나요?**

등록 시 법인명(사업부명)으로 1개 등록하면 됩니다. 법인이 1개인 경우, 2개 회사의 고유식별정보 보유량 및 자체점검 결과를 통합하여 조사에 참여해 주시면 됩니다.

Q6	**계열사 5개의 개인정보처리시스템을 통합 관리합니다. 조사 결과를 계열사별로 등록해야 하나요?**

계열사가 개인정보처리시스템을 접속하여 조회만 가능하며 실제 데이터는 그룹 내 DB에서 보유·처리할 경우, 해당 기업만 등록하면 됩니다.

Q7	**본 기업이 대기업, 중견기업, 중소기업 중 어디에 속하는지요?**

자산규모, 매출액, 상시근로자 수, 업종에 따라 차이가 있을 수 있으니 정확한 사항은 법제처에서 아래 사항을 검색하여 확인해보시고 기업에서 파악하여 유형2 또는 유형3을 선택해 주시면 됩니다.

"대기업"이란 「독점규제 및 공정거래에 관한 법률」 제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
"중견기업"이란「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」제2조에 해당하는 기업을 말한다.
"중소기업"이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.

Q8	**기관현황 등록 시 유형 2 또는 유형 3 기준은 어떻게 적용하여야 하나요?**

기관현황 등록 시점 기준, 고유식별정보를 포함하여 기관 내에서 보유하고 있는 정보주체에 대한 개인정보 보유량을 기준으로 합니다, (중소기업 기준) 100만 명 미만일 경우 유형2, 100만 명 이상일 경우 유형3으로 선택합니다.

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



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

Q9	**개인정보처리시스템 중 점검 진행해야 하는 시스템은 어느 것인가요?**

대상기관에서 사용하시는 개인정보처리시스템 중 고유식별정보를 처리하는 시스템만 자체점검 결과 및 증빙자료를 제출해주시면 됩니다.

Q10	**고유식별정보가 포함된 개인정보처리시스템 등록 기준은 무엇인가요? 개인정보처리시스템 보유 기준은 무엇인가요?**
대상기관에서 서버 등을 직접 운영·관리(외부 위탁 운영 포함)하는 개인정보처리시스템이 있고, 해당 처리시스템에 고유식별정보가 포함되어 있다면 '기관현황 – 고유식별정보가 포함된 개인정보처리시스템'에 등록하여야 합니다. 이 경우 총 26개 항목에 대하여 점검을 진행하며, 서버 등을 직접 운영·관리(외부 위탁 운영 포함)하는 개인정보처리시스템이 없는 경우에는 개인정보처리시스템 '미보유'에 해당하여 총 9개 항목에 대하여 점검을 진행합니다.	

Q11	**그룹웨어, ERP, 개인별 인사시스템을 고유식별정보 처리시스템으로 볼 수 있나요?**
그룹웨어 시스템은 고유식별정보 처리시스템은 아니며, ERP와 개인별 인사시스템에서 팀장이 팀원의 주민등록번호가 포함된 인사 프로필을 조회하는 경우라면 고유식별정보 처리시스템으로 봅니다.	

Q12	**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. 미조치된 시스템에 대하여서는 조치를 완료한 이후 결과를 입력하시는 것이 바람직합니다.	

Q13	**주민등록번호가 생년월일만 있는 경우, 고유식별정보인가요? 또, 주민등록번호 일부가 마스킹(예: 901122-1******) 등으로 표시되어있는 경우도 고유식별정보인가요?**
최초 정보를 수집할 때 생년월일만 수집한다면 고유식별정보가 아닙니다. 다만 수집 이후 암호화 및 마스킹 처리가 되어있더라도 원래 데이터로 복원이 가능한 정보일 경우에는 고유식별정보에 해당합니다.	

Q14	**고유식별정보 보유현황 산정 시 한 명에 대한 주민등록번호, 운전면허번호가 적힌 서류가 있다면 이것은 2건으로 처리하나요?**
한 명에 대한 주민등록번호와 운전면허번호가 각각 적힌 서류의 경우, 2건의 고유식별정보로 산정합니다.	

Q15	**동일 DB 상의 고유식별정보가 여러 Table에 있을 시 중복포함 또는 중복제거 되어야 하나요?**
동일 DB 상의 여러 Table에 고유식별정보를 보유할 경우 별도로 1건씩 산정합니다.	

Q16	**업무용 PC 고유식별정보 보유량 산정은 어떻게 하나요?**
업무용 PC의 파일에 고유식별정보가 포함된 경우, 파일의 개수가 아닌 파일에 포함된 보유량을 파악해야 합니다. 다만 엑셀파일에서 replace 함수를 사용하여 마스킹 되어있더라도 원래 데이터로 복원이 가능한 정보일 경우에는 고유식별정보 보유량에 산정합니다.	

Q17	**올해 조사에 참고하기 위해 이전 자료를 전달받을 수 있나요?**
이전에 고유식별정보 안전조치 관리실태 조사에 참여했던 기관에 한하여 이전 자료를 전달받을 수 있으며, 조사 당시 담당자의 정보(성명 및 담당 부서 등)를 확인 후 메일로 보내드릴 수 있습니다.	

Q18	**안전조치 자체점검 시 세부 조치방법 등에 대하여 조사 매뉴얼을 참고하여도 잘 이해가 되지 않아 어려움이 있습니다. 이런 경우 도움을 얻을 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 때는 안전조치 무료 현장컨설팅을 신청하실 수 있습니다. ※ 문의처 : 고유식별정보 안전조치 관리실태 조사 사무국(이메일 unique@finss.co.kr, 유선 1800-8671) ※ 현장컨설팅의 경우 선착순 일부 기관에 한하여 무료로 제공하며, 신청방법은 고유식별정보 안전조치 관리실태 조사 사무국으로 문의	

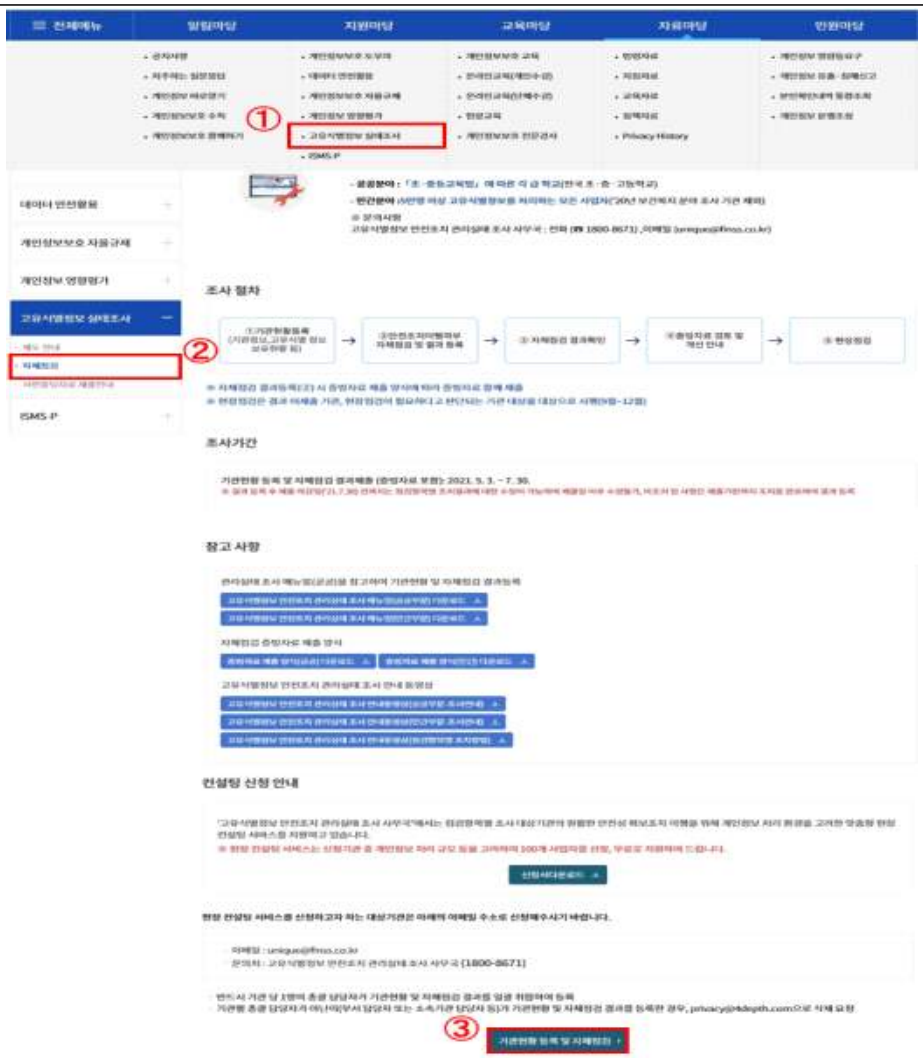
Q19	**현장 컨설팅 접수 방법은 어떻게 되나요? 현장 컨설팅을 받게 될 경우, 지속적인 감시 대상이 되거나 행정처분의 대상이 되지는 않나요?**
현장 컨설팅은 고유식별정보 관리실태 조사에 관한 상담뿐만 아니라 개인정보보호 관련 전반적인 사항에 관한 상담을 무료로 방문하여 진행하고 있으며, 접수 방법은 개인정보보호 종합지원시스템·개인정보보호 포털 사이트 내에 신청서 양식을 내려받은 후 조사 사무국 이메일로 신청서를 보내주시면 됩니다. 현장 컨설팅은 감사의 목적이 아니라 지원의 목적이기 때문에 컨설팅 이후 지속적인 관리·감시 대상이 된다거나 미비한 사항 적발 시 행정처분을 내리는 등의 불이익은 없습니다.	

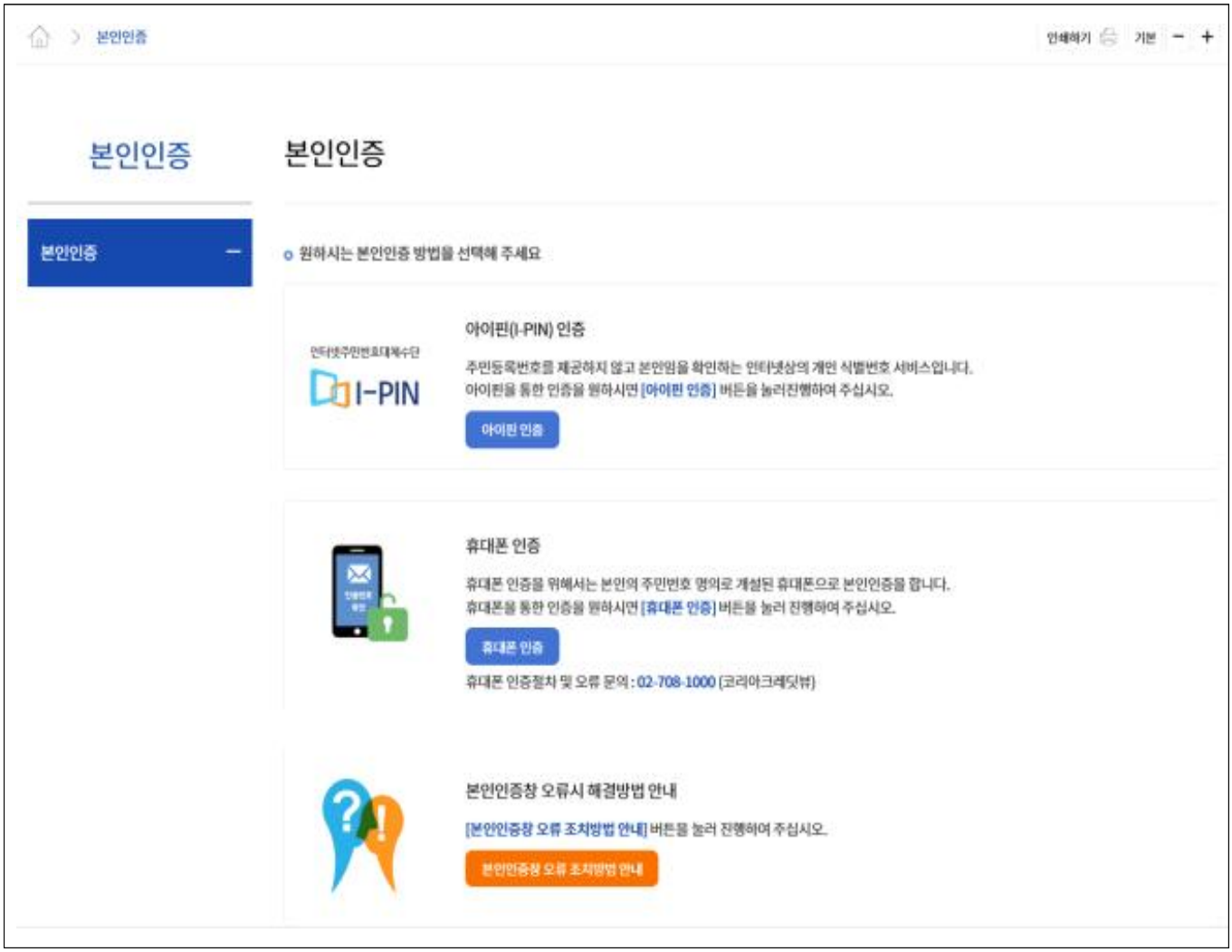
Q20	**조사 중 담당자 변경, 조사 결과등록 오류 등 개인정보보호 종합지원시스템·개인정보보호 포털 내 문제 시 어디에 문의해야 하나요?**
조사 중 담당자 변경, 조사 결과등록 오류 등 개인정보보호 종합지원시스템·개인정보보호 포털 내 문제 발생 시에는 **시스템 업체(02-6952-8650)**에 연락하여 해당 내용 요청 후, 재조사를 진행하시면 됩니다.	

4 시스템 사용 방법

4-1 담당자 등록 방법

※ 기관현황 등록사항은 대상기관 담당자 1명이 일괄 등록합니다.

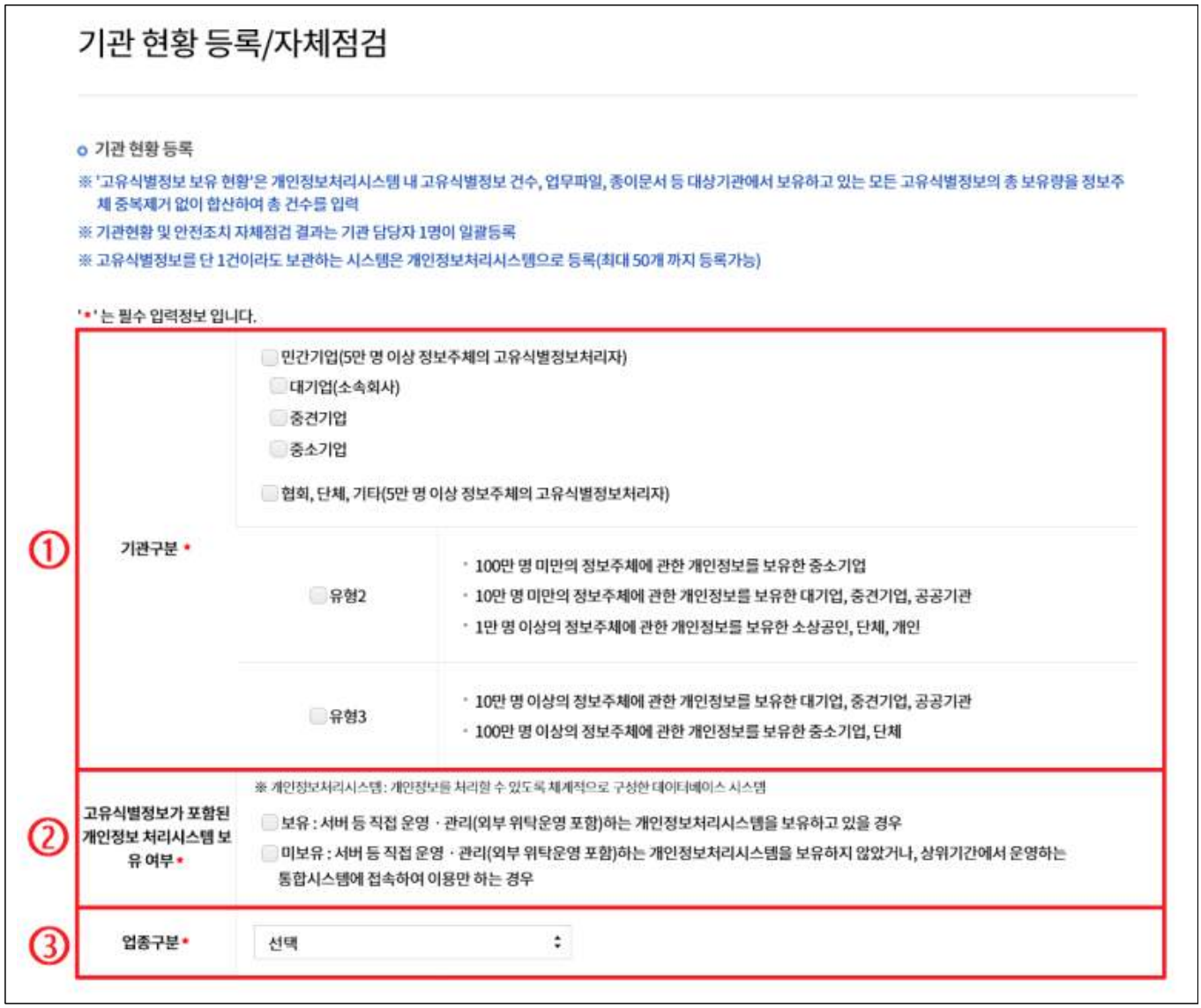




④ 본인인증 화면이 나타나면 아이핀 또는 휴대폰 인증을 진행합니다.
인증의 경우 기관의 개인정보 담당자가 받도록 하며, 추후 지속적으로 접근할 수 있는 담당자가 인증 받도록 합니다.

⑤ 본인인증 절차가 완료되면, 기관현황 등록페이지로 전환됩니다.

4-2 기관현황 등록 방법



① 기관구분

: 민간부문 해당 시 대기업, 중견기업, 중소기업 중 선택하여 입력하고, 그렇지 않을 경우 협회, 단체, 기타를 선택합니다. '유형 2' 또는 '유형 3' 중에서 설명내용에 맞는 유형을 선택합니다.

※ 대기업이란 「독점규제 및 공정거래에 관한 법률」 제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.

※ 중견기업이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조에 해당하는 기업을 말한다.

※ 중소기업이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.

참고사항

■ 민간부문의 구분('21년 3월 현재 기준)
- (대기업, 중견기업, 중소기업) **20년 개인정보의 안전성 확보조치 기준 해설서 19p~22p 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」(고시)
[참고] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준 참조

② 고유식별정보가 포함된 개인정보처리시스템 보유 여부
: 외부 위탁 운영을 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.

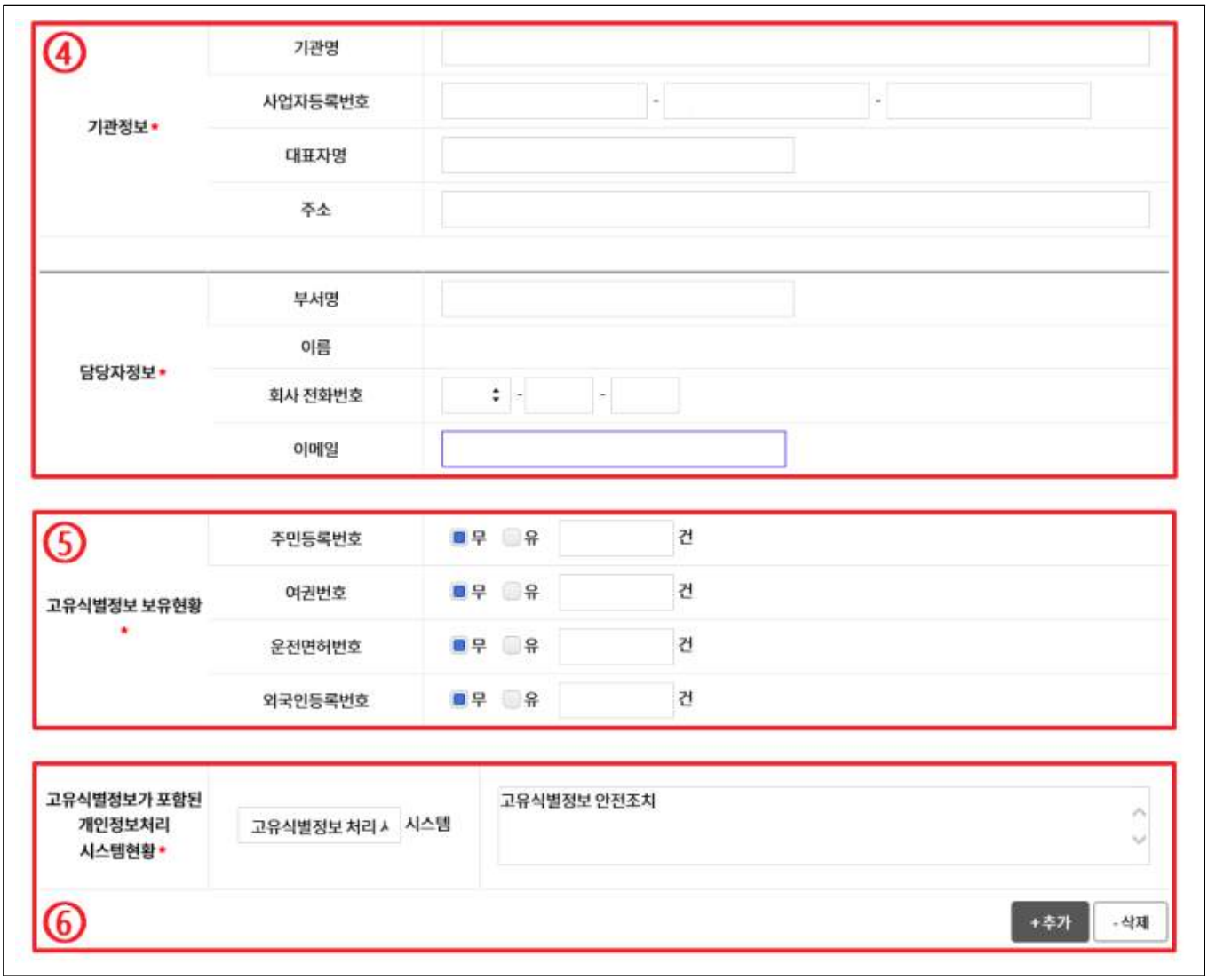
■ 업무용 컴퓨터의 경우에도 데이터베이스 응용프로그램이 설치·운영되어 다수의 개인정보취급자가 개인정보를 처리하는 경우에는 개인정보처리시스템에 해당될 수 있음. 다만, 데이터베이스 응용프로그램이 설치·운영되지 않는 PC, 노트북과 같은 업무용 컴퓨터는 개인정보처리시스템에서 제외.

③ 업종구분

: 대상기관이 해당하는 업종을 선택하여 입력합니다.

※ 통계청: 한국표준산업분류의 대분류 참고

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



④ 기관정보 및 담당자 정보

: 기관명(회사명), 사업자등록번호, 대표자명, 회사 주소에 대하여 입력합니다. 대상기관 실태조사 담당 직원의 부서명, 성명, 회사전화번호, 이메일주소를 입력합니다.

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

⑤ 고유식별정보 보유현황

: 대상기관에서 현재 보유하고 있는 고유식별정보의 종류와 건수를 입력합니다.

※ 한 사람의 고유식별정보가 여러 곳에 중복되는 경우 별도로 1건씩 산정

(예: 홍길동의 주민등록번호가 A시스템, B시스템, C종이문서에 존재 → 주민등록번호 3건)

※ 한 사람의 고유식별정보 2종류를 보유하고 있을 경우 별도로 1건씩 산정

(예: 홍길동의 주민등록번호, 여권번호 보유 시 → 주민등록번호 1건, 여권번호 1건)

※ 고유식별정보 보유 건수는 임직원의 정보도 포함하여 산정

⑥ 고유식별정보가 포함된 개인정보처리시스템 현황

: ②번 항목에서 개인정보처리시스템 미보유 선택 시에는 비활성화됩니다. 대상기관이 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 보유 여부(보유・미보유)에 따라 자체점검 항목에 차이가 있으므로, 기관현황 등록이 완료되어야만 자체점검을 진행함. 해당 사항에 대하여 충분히 파악한 이후 기관현황 등록을 진행하여 주시기 바라며, **기관현황은 등록이 완료된 이후에도 '21. 7. 30.(금)까지 자체점검 결과와 함께 수정할 수 있음.**

4-3 자체점검 제출 방법



기관 현황 등록/자체점검

고유식별정보 안전조치 자체점검

번호	세부 점검내용	조치 (있음)	미조치 (없음)	해당 없음	도움말
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				
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 개인정보처리 시스템에 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				

① 기관 현황 등록 절차가 완료되면 자체점검 등록페이지로 전환되며, 자체점검 페이지가 나타나면 세부 점검내용을 읽어보며, 기관 내 점검항목 조치 여부에 대해 담당자가 판단하여 조사를 진행합니다.

※ 이해하기 어려운 항목에 대해서는 우측 도움말을 참고하여 조사 진행

② 자체점검 조사가 완료되면 하단 증빙자료 제출을 진행합니다. **자체점검 조사는 증빙자료 첨부까지 진행하셔야 조사가 마무리 됩니다.**

참고사항



■ 증빙자료 미첨부 상태로 자체점검 저장시 등록이 완료되지 않음

4-4 증빙자료 제출 방법

※ 증빙자료 제출은 고유식별정보 보유량이 가장 많은 대표 시스템(개인정보처리시스템) 1개만을 대상으로 진행

※ 고유식별정보 안내 페이지에서 '증빙자료 제출 양식'을 미리 내려받아 작성

※ 웹 브라우저가 '팝업 차단'이 되어있다면 '팝업 차단 해체' 필요



① 자체점검 절차가 완료되면, 자체점검을 진행한 페이지 하단의 '증빙자료'를 확인 후 [+추가] 버튼을 클릭합니다.

※ 증빙자료 제출 화면 상단에서도 증빙자료 제출 양식을 내려받기 가능



② '증빙자료 업로드' 팝업화면이 나타나면, '증빙자료 업로드' 항목에 있는 [파일추가] 버튼을 눌러 증빙자료를 시스템에 업로드합니다.

※ PDF(.pdf), 한글(.hwp) 문서만 등록 가능

③ [전송하기]를 눌러 파일을 업로드하면, 증빙자료 제출이 완료됩니다.

④ [닫기]를 누르고 나와, 자체점검을 진행한 페이지 하단의 [자체점검 등록] 버튼을 클릭하면 조사가 마무리됩니다.

4-5 수정 방법

❑ 담당자 정보 수정 방법

※ 담당자 정보에 대한 수정 요청은 **시스템 업체(02-6952-8650)**에서 요청.
담당자 정보 수정 시, 기관현황 등록 및 자체점검, 증빙자료 또한 일괄 삭제.

❑ 기관현황 등록 수정 방법

※ 수정 가능기간: 등록이후 ~ 제출일 ('21. 7. 30.)전까지

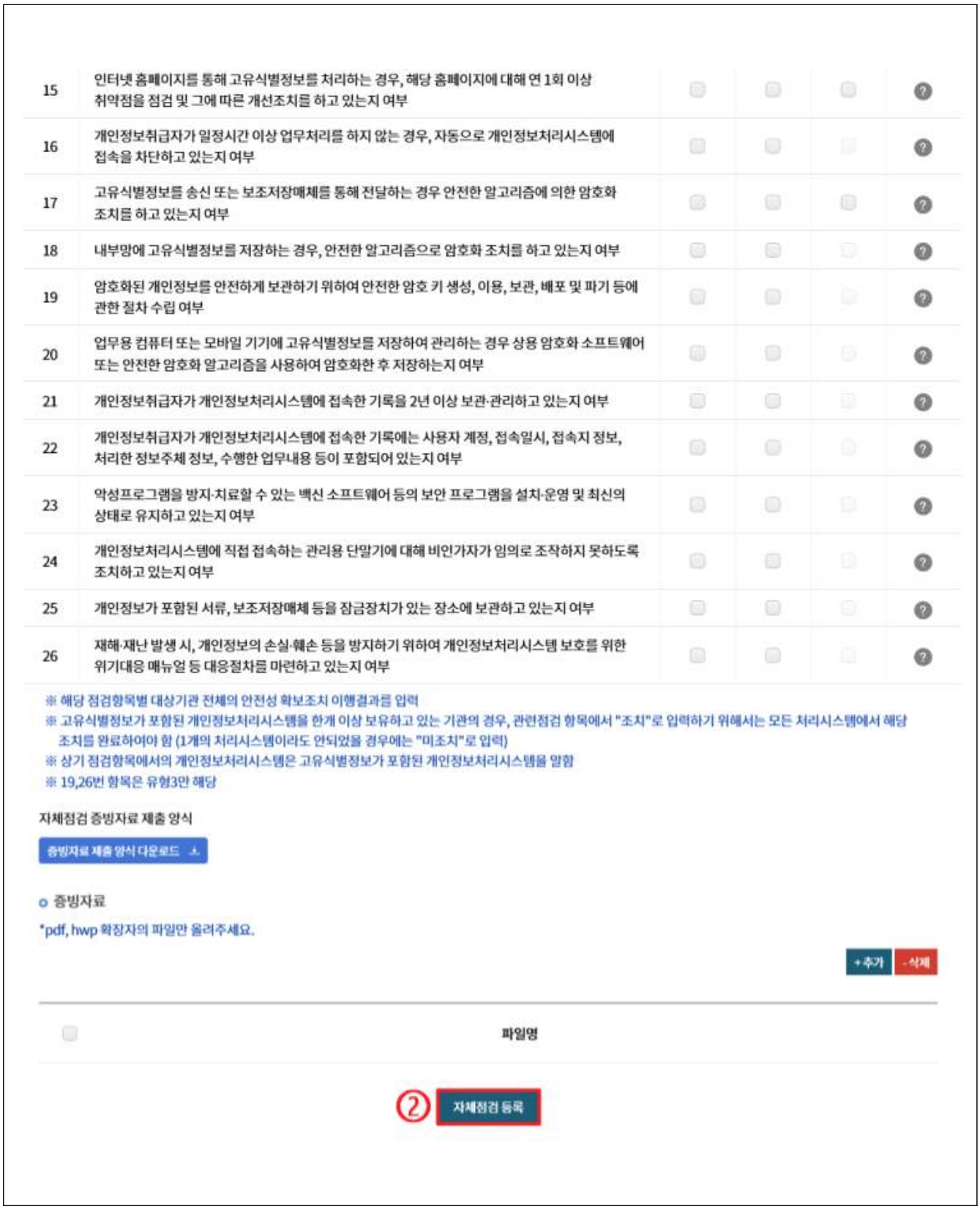


① 개인정보보호 포털 → 고유식별정보 실태조사 안내(기관현황/자체점검) → 본인인증 후, 등록된 기관현황 정보 및 자체점검 결과를 수정 가능합니다.

❑ 자체점검 수정 방법



① 자체점검 등록 현황 페이지로 들어가, 우측 하단의 [수정] 버튼을 클릭합니다.



② 기존에 입력한 자체점검 결과에 대하여 수정을 진행하고, 페이지 하단의 [자체점검 등록] 버튼을 클릭하여 조사를 마무리합니다.

❑ 증빙자료 수정 방법



① 자체점검 등록 현황 페이지로 들어가 제출한 증빙자료를 확인하고, 하단의 [수정] 버튼을 클릭합니다.



② 증빙자료 수정을 위하여 하단의 '증빙자료'를 확인 후 수정을 원하는 파일에 대해 [-삭제] 버튼을 클릭하여 삭제하고, 좌측의 [+추가] 버튼을 클릭합니다.



③ '증빙자료 업로드' 팝업화면이 나타나면, '증빙자료 업로드' 항목에 있는 [파일추가] 버튼을 눌러 증빙자료를 시스템에 업로드합니다.

※ PDF(.pdf), 한글(.hwp) 문서만 등록 가능

④ [전송하기]를 눌러 파일을 업로드하면, 증빙자료 제출이 완료됩니다.

⑤ [닫기]를 누르고 나와, 페이지 하단의 [자체점검 등록] 버튼을 클릭하여 수정을 마무리 합니다.

5 점검방법

5-1 전체 점검항목

※ 개인정보처리시스템 미보유 시 점검항목 : 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
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)

※ 유형2 : 점검항목 19, 26번을 점검하지 않음
※ 유형3 : 26가지 항목 모두 점검
※ 유형2, 유형3 기준

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

5-2 증빙자료 제출 점검항목

※ 증빙자료 제출은 고유식별정보 보유량이 가장 많은 대표 시스템(개인정보처리시스템) 1개만을 대상으로 진행

❑ 개인정보처리시스템 보유 시 증빙자료 제출 점검항목

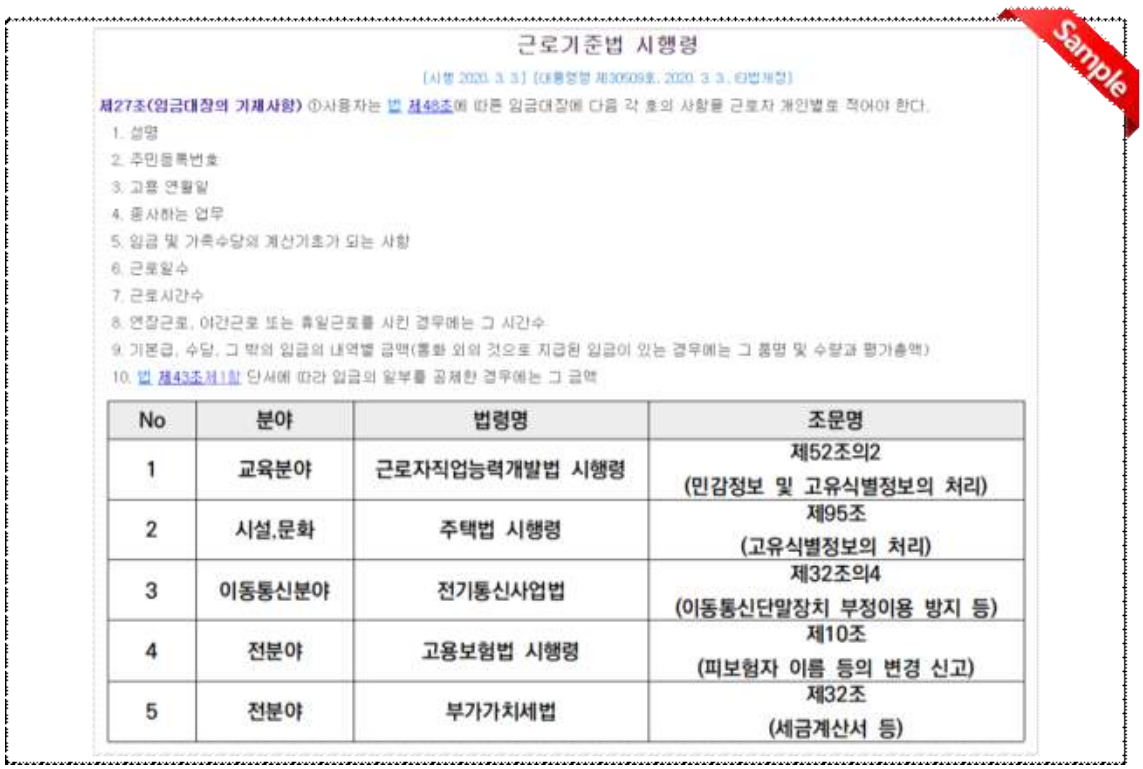
⑥	전보 또는 퇴직 등 개인정보취급자 변경 시, 개인정보처리시스템에 대한 접근권한을 변경 또는 말소하고 있는지 여부
⑩	사용자계정 또는 비밀번호를 일정 횟수이상 잘못 입력한 경우, 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는지 여부
⑬	외부에서 개인정보처리시스템에 접속 시, 가상사설망(VPN), 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하고 있는지 여부
⑯	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 개인정보처리시스템에 접속을 차단하고 있는지 여부
⑱	내부망에 고유식별정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는지 여부
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
㉓	악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영 및 최신의 상태로 유지하고 있는지 여부

❑ 개인정보처리시스템 미보유 시 증빙자료 제출 점검항목

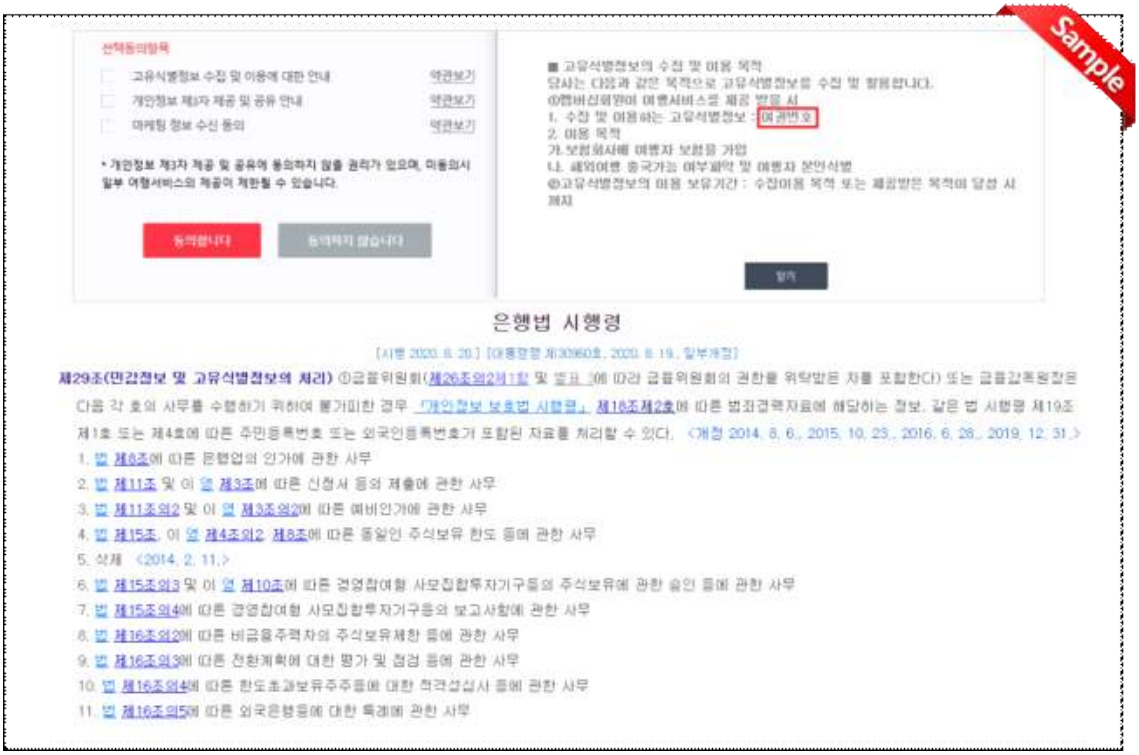
④	개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행하고 있는지 여부
㉕	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 장소에 보관하고 있는지 여부

5-3 점검항목 세부안내

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 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 보호위원회가 고시로 정하는 경우
점검 방법	1. 주민등록번호 처리 여부 확인 1) 대상기관에서 주민등록번호를 처리(수집·이용·제공 등)하는지 여부를 확인합니다. 2. 주민등록번호를 처리하는 적절한 법령을 제시 1) OO법 O조 O항 (고유식별정보의 처리) 등 대상기관의 적절한 법령을 확인합니다. 2) 주민등록번호 수집 법정주의로 인해 주민등록번호는 정보주체의 동의를 받아도 처리할 수 없습니다.
점검 기준	◦ 미조치 : 주민등록번호를 처리하나 법령 근거가 없는 경우 ◦ 해당없음 : 주민등록번호를 처리하지 않는 경우
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p170~173

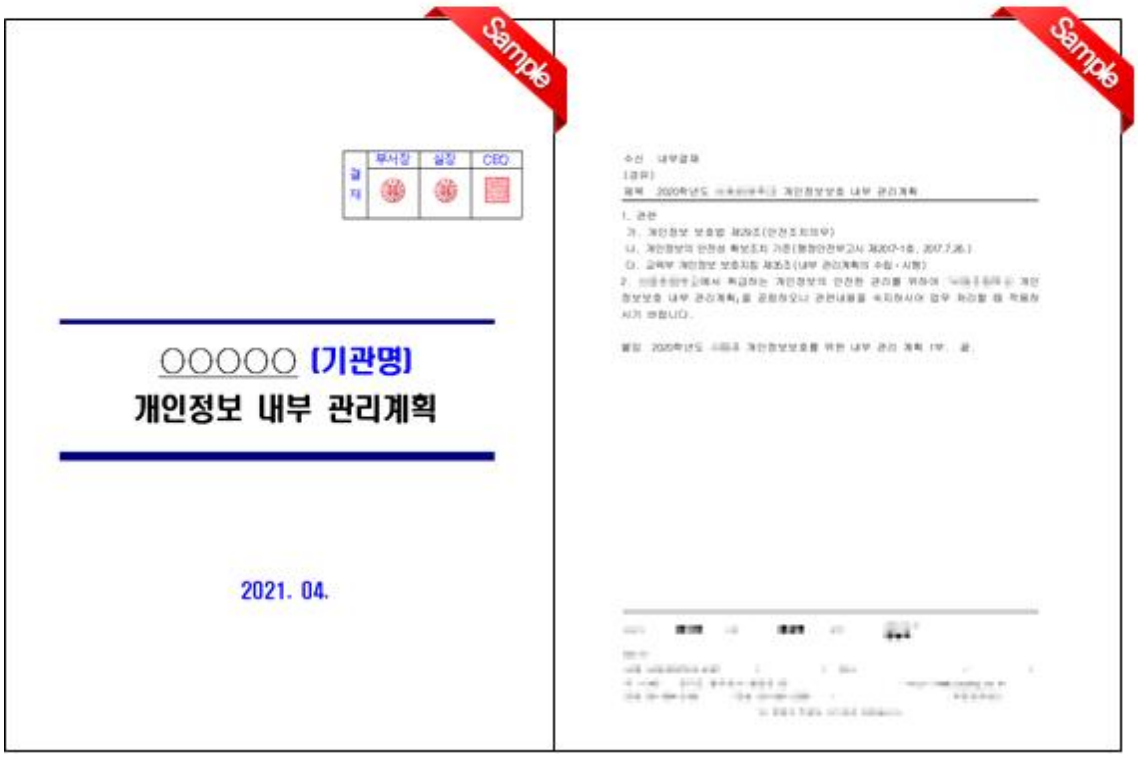


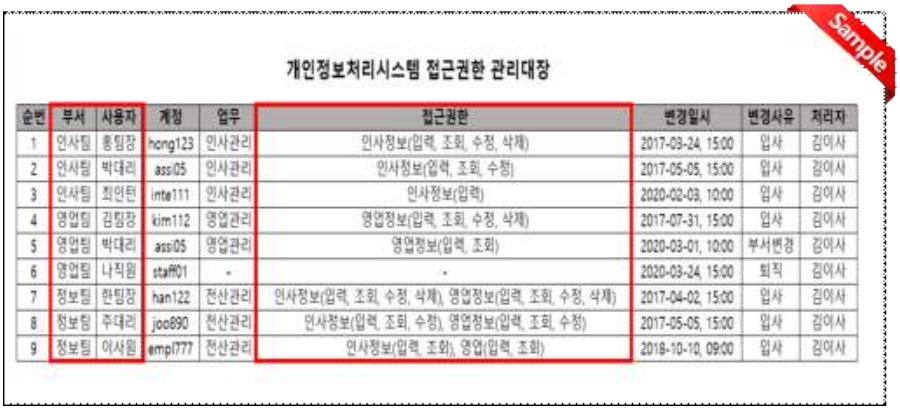
No	분야	법령명	조문명
1	교육분야	근로자직업능력개발법 시행령	제52조의2 (민감정보 및 고유식별정보의 처리)
2	시설,문화	주택법 시행령	제95조 (고유식별정보의 처리)
3	이동통신분야	전기통신사업법	제32조의4 (이동통신단말장치 부정이용 방지 등)
4	전분야	고용보험법 시행령	제10조 (피보험자 이름 등의 변경 신고)
5	전분야	부가가치세법	제32조 (세금계산서 등)

2	**여권번호, 운전면허번호, 외국인등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거 또는 정보주체의 동의가 있는지 여부**
관련 규정	**개인정보보호법 제24조(고유식별정보의 처리 제한)** **→ 고유식별정보(여권번호, 운전면허번호, 외국인등록번호)를 적절한 법령에 따라 처리하는지 여부 확인** 1. 정보주체에 동의를 받은 경우 2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우
점검 방법	1. 고유식별정보(여권번호, 운전면허번호, 외국인등록번호)를 처리 여부 확인 1) 대상기관에서 고유식별정보를 처리(수집・이용・제공 등)하는지 여부를 확인합니다. 2. 고유식별정보를 처리하는 적절한 법령을 제시 1) 별도의 동의를 받는 경우 확인합니다.(주민등록번호 제외) 2) 고유식별정보를 처리할 수 있는 적절한 법령을 확인합니다. 
점검 기준	◦ 미조치 : 고유식별정보를 처리하나 법령 근거가 없거나, 정보주체의 별도 동의를 받지 않는 경우 ◦ 해당없음 : 고유식별정보를 처리하지 않는 경우
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p165~169

3	수집목적이 달성되었고, 보존기간이 경과한 고유식별정보를 파기하고 있는지 여부
관련 규정	**개인정보보호법 제21조(개인정보의 파기)** **→ 수집목적이 달성되었거나, 보존기간이 지난 고유식별정보 파기 여부 확인** 1. 보존기간의 경과, 개인정보의 처리목적 달성 등 그 개인정보가 불필요하게 되었을 때는 지체없이 개인정보를 파기(다만, 법령에 따라 보존해야 하는 경우 제외) 2. 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치 3. 개인정보를 파기하지 않고 보존해야 하는 경우에는 해당 개인정보를 다른 개인정보와 분리하여 저장・관리
점검 방법	1. 고유식별정보 수집목적에 따른 보존기간 확인 1) 수집한 고유식별정보의 보존기간을 확인하고 보존기간이 지난 고유식별정보가 존재하는지 확인합니다. 2. 고유식별정보 파기 여부 확인 1) 고유식별정보 보존기간이 경과된 경우 보존기간 종료일로부터 지체없이 파기를 수행하고 있는지 확인합니다.  <파기방법> 2) 개인정보 보호책임자는 수집목적이 달성되거나 보존기간이 지난 개인정보의 파기를 점검·관리해야 합니다. 3) 다만, 법령에 따라 보존하여야 하는 경우 기존 개인정보파일과 분리하여 별도 보관하여야 합니다.
점검 기준	◦ 미조치 : 보존기간이 지난 고유식별정보가 존재하는 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p137~143 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p121

4	개인정보의 안전한 처리를 위한 내부관리계획을 수립·시행하고 있는지 여부
① 개인정보처리시스템 미 보유 기관 증빙자료 제출 항목(1/2)	
관련 규정	**개인정보의 안전성 확보조치 기준 제4조(내부관리계획의 수립・시행)** **→ 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 필수사항을 포함하는 내부관리계획을 수립·시행하는지 여부 확인**
점검 방법	1. 내부관리계획 시행 여부 확인 1) 개인정보의 안전한 처리를 위해 개인정보 보호책임자의 의무와 책임, 개인정보 처리단계별 기술적・관리적 안전조치, 개인정보 교육, 개인정보 침해대응 및 피해구제 등과 같은 개인정보보호 의무를 위한 내부관리계획서 수립・시행 여부를 확인합니다. 2) 내부관리계획이라는 명칭 이외의 다른 명칭(예: 개인정보보호지침 등)으로 수립하여도 내부관리계획의 필수 반영사항이 모두 포함된 경우 내부관리계획으로 인정됩니다. ※ 내부관리계획 필수사항(유형2일 시 필수항목 12-14번을 포함하지 않을 수 있음) 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 3) 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리해야 합니다.
점검 기준	◦ 미조치 : 내부관리계획을 수립하지 않거나 문서화하지 않은 경우 ◦ 해당없음 : 없음

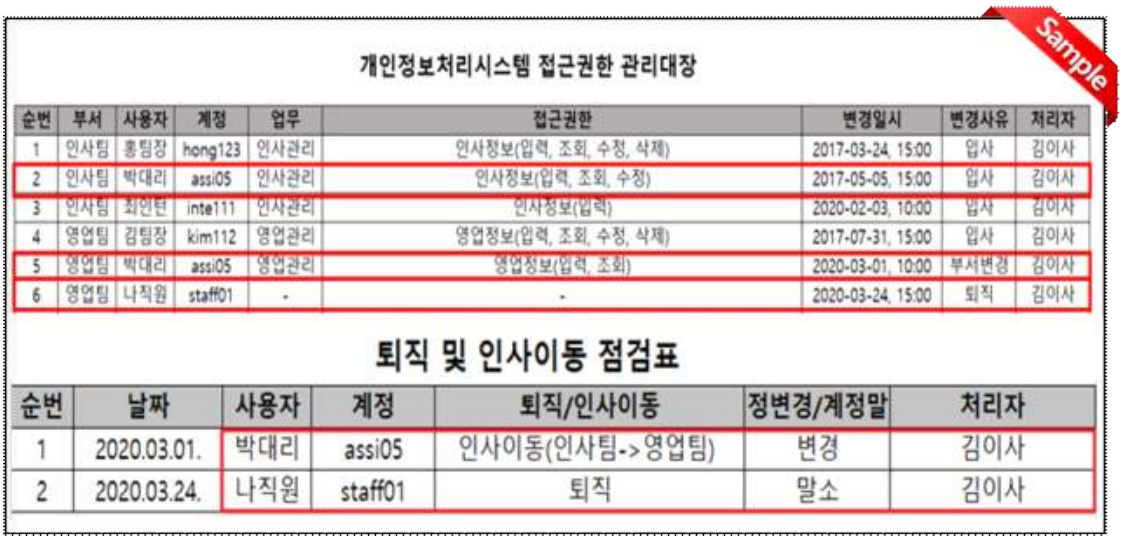
증빙 자료	**1. 내부관리계획 표지 내 최고경영층 승인 또는 내부관리계획 수립 및 시행 기안서 <필수>** 
참고 자료	개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p33~45

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 부여하는지 확인 2. 업무처리 방법(조회, 생성, 변경 삭제 등)에 따라 접근권한 부여하는지 확인 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법	1. 해당 기관의 개인정보취급자 식별 1) 개인정보처리시스템에 접근 가능한 개인정보취급자(담당자)를 확인합니다. 2. 기관 내 식별된 개인정보취급자의 담당업무에 적합한 개인정보처리시스템 접근권한 부여 확인 1) 식별된 개인정보취급자의 업무 목적에 적합하게 최소한의 범위로 접근권한이 부여되어 있는지 접근권한 관리 테이블을 확인합니다.  사용자 권한관리 (Sample) 부서명 / 권한상태 조회결과 부서 | 직책 | 사용자 | 계정 | 업무 | 접근권한 | 변경일시 | 변경사유 | 처리자 인사팀 | 팀장 | 김OO | INSA1 | 인사관리 | 인사정보 (입력, 조회, 수정, 삭제) | 2018-04-17, 13:00 | 승진 | 김이사 인사팀 | 대리 | 이OO | INSA2 | 인사관리 | 인사정보 (입력,조회, 수정) | 2018-05-13, 14:05 | 부서변경 | 김이사 인사팀 | 사원 | 박OO | INSA3 | 인사관리 | 인사정보(입력) | 2019-02-13, 10:20 | 입사 | 김이사 영업팀 | 팀장 | 최OO | SALES1 | 영업관리 | 영업정보 (입력, 조회, 수정, 삭제) | 2019-04-19, 17:00 | 승진 | 김이사 영업팀 | 대리 | 정OO | SALES2 | 영업관리 | 영업정보(입력, 조회) | 2020-06-07, 16:00 | 입사 | 김이사 영업팀 | 사원 | 강OO | SALES3 | 영업관리 | - | 2021-02-22, 11:07 | 퇴사 | 김이사 2) 개인정보처리시스템에 기능이 없다면 수기문서로 관리하도록 합니다.  개인정보처리시스템 접근권한 관리대장 (Sample) 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 | ass05 | 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 | ass05 | 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
점검 기준	◦ 미조치 : 개인정보처리시스템 접근권한을 차등 부여하지 않을 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p263 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p47

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

① 개인정보처리시스템 보유 기관 증빙자료 제출 항목(1/8)

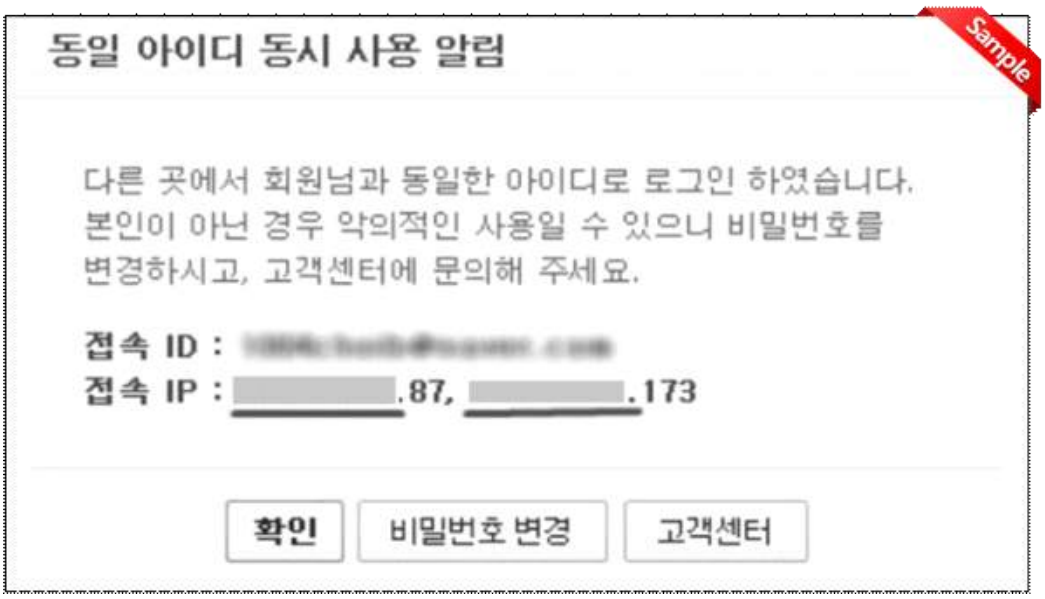
관련 규정	**개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)** **→ 개인정보취급자의 전보 또는 퇴직 등 인사이동 발생 시 개인정보처리시스템의 접근권한을 즉시 변경 또는 말소하는지 확인** 1. 직원의 퇴직 시 해당 직원의 계정을 지체없이 변경·말소하는 조치 등을 내부관리계획 등에 반영하여 이행 2. 직원의 퇴직 시 계정 말소를 효과적으로 이행하기 위해서는 퇴직 점검표에 사용자계정의 말소 항목을 반영하여, 계정 말소 여부에 대해 확인 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법	1. 내부관리계획 내 접근권한 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. 2) 계정 말소를 효과적으로 이행하기 위해서 퇴직 및 인사이동 점검표에 사용자 계정 말소 항목을 반영하여, 계정 말소에 대한 확인을 받을 수 있습니다. 
점검 기준	◦ 미조치 : 퇴직 및 인사이동 후 개인정보처리시스템 접근권한을 변경·말소하지 않는 경우 ◦ 해당없음 : 없음

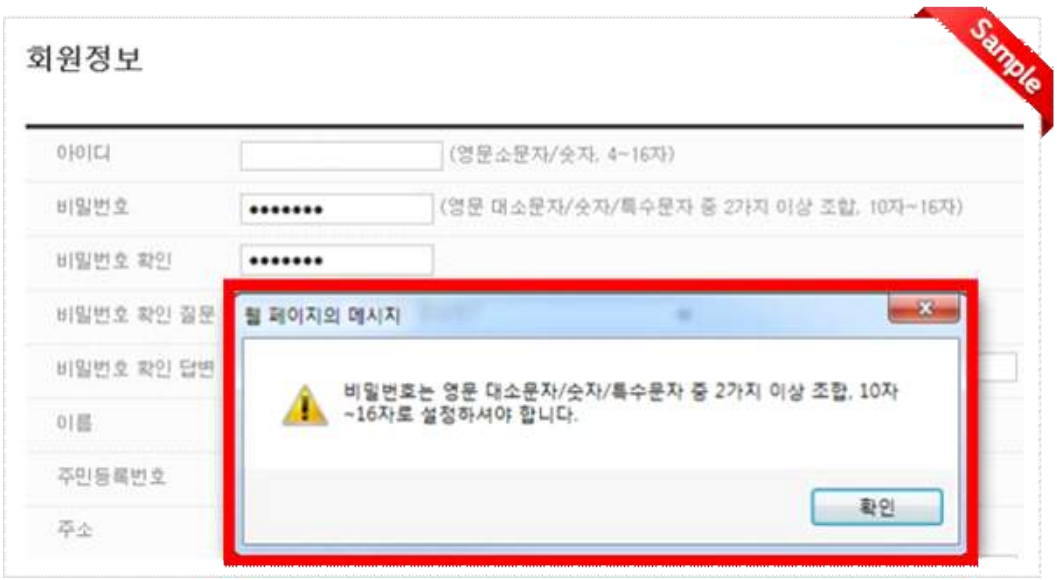
증빙 자료	**1. 접근권한이 변경·말소된 기록을 확인할 수 있는 접근권한 시스템 화면 <필수>**  사용자 권한관리 Sample 부서명 권한상태 반려포함 반려제외 조회결과 부서 직책 사용자 계정 업무 접근권한 변경일시 변경사유 처리자 인사팀 팀장 김OO INSA1 인사관리 인사정보 (입력, 조회, 수정, 삭제) 2018-04-17, 13:00 승진 김이사 인사팀 대리 이OO INSA2 인사관리 인사정보 (입력,조회, 수정) 2018-05-13, 14:05 부서변경 김이사 인사팀 사원 박OO INSA3 인사관리 인사정보(입력) 2019-02-13, 10:20 입사 김이사 영업팀 팀장 최OO SALES1 영업관리 영업정보 (입력, 조회, 수정, 삭제) 2019-04-19, 17:00 승진 김이사 영업팀 대리 정OO SALES2 영업관리 영업정보(입력, 조회) 2020-06-07, 16:00 입사 김이사 영업팀 사원 강OO SALES3 영업관리 - 2021-02-22, 11:07 퇴사 김이사 **2. 시스템 내 기능이 없는 경우, 수기 문서 관리대장 <필수>**  Sample 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 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
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p263 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p47 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p22

<table>
<tr><td>7</td><td>개인정보처리시스템에 대한 개인정보취급자의 접근권한 부여·변경·말소 내역을 기록하고 있으며 3년간 보관하고 있는지 여부</td></tr>
<tr><td>관련 규정</td><td>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</td></tr>
<tr><td>점검 방법</td><td>1. 해당 개인정보처리시스템 구축 이후 최소 3년간 접근권한 부여·변경·말소 내역 기록 여부 확인
1) 해당 개인정보처리시스템에 접근권한 변경 기록이 구축 이후 최소 3년간 기록되고 있는지 확인합니다.

사용자 권한관리
부서명 권한상태
조회결과
부서 직책 사용자 계정 업무 접근권한 변경일시 변경사유 처리자
인사팀 팀장 김OO INSA1 인사관리 인사정보 (입력, 조회, 수정, 삭제) 2018-04-17, 13:00 승진 김이사
인사팀 대리 이OO INSA2 인사관리 인사정보 (입력,조회, 수정) 2018-05-13, 14:05 부서변경 김이사
인사팀 사원 박OO INSA3 인사관리 인사정보(입력) 2019-02-13, 10:20 입사 김이사
영업팀 팀장 최OO SALES1 영업관리 영업정보 (입력, 조회, 수정, 삭제) 2019-04-19, 17:00 승진 김이사
영업팀 대리 정OO SALES2 영업관리 영업정보(입력, 조회) 2020-06-07, 16:00 입사 김이사
영업팀 사원 강OO SALES3 영업관리 - 2021-02-22, 11:07 퇴사 김이사
2) 개인정보처리시스템에 기능이 없다면 수기문서로 관리하도록 합니다.

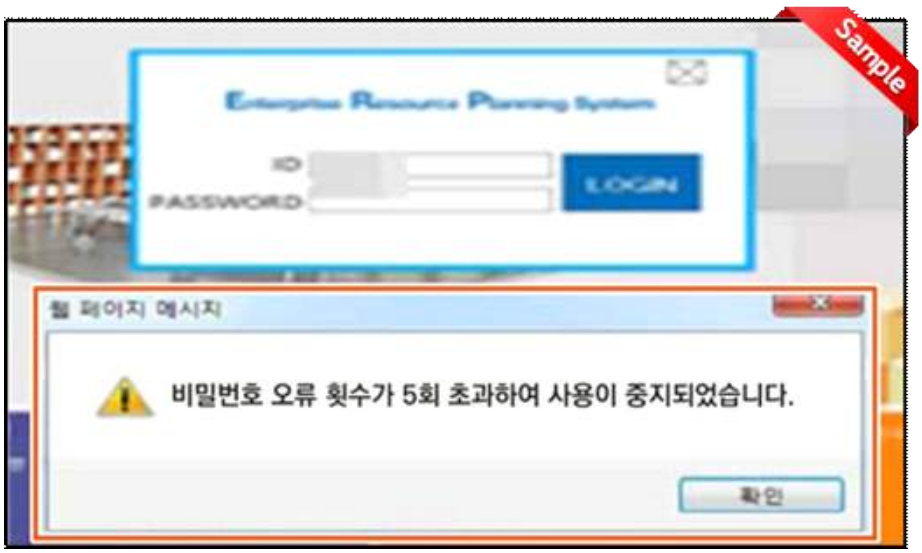
개인정보처리시스템 접근권한 관리대장
순번 부서 사용자 계정 업무 접근권한 변경일시 변경사유 처리자
1 인사팀 홍팀장 hong123 인사관리 인사정보(입력, 조회, 수정, 삭제) 2017-03-24, 15:00 입사 김이사
2 인사팀 박대리 assi05 인사관리 인사정보(입력, 조회, 수정) 2017-05-05, 15:00 입사 김이사
3 인사팀 최인턴 inte111 인사관리 인사정보(입력) 2020-02-03, 10:00 입사 김이사
4 영업팀 김팀장 kim112 영업관리 영업정보(입력, 조회, 수정, 삭제) 2017-07-31, 15:00 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) 2017-05-08, 15:00 입사 김이사
9 정보팀 이사원 empl777 전산관리 인사정보(입력, 조회), 영업정보(입력, 조회) 2018-10-10, 09:00 입사 김이사</td></tr>
<tr><td>점검 기준</td><td>◦ 미조치 : 접근권한 부여·변경·말소 내역을 기록하지 않거나 3년간 보유하지 않는 경우
◦ 해당없음 : 없음</td></tr>
<tr><td>참고 자료</td><td>개인정보보호위원회, “개인정보보호 법령 및 지침·고시 해설서(2020.12)”, p263
개인정보보호위원회, 한국인터넷진흥원, “개인정보의 안전성 확보조치 기준 해설서(2020.12)”, p48</td></tr>
</table>

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 확인 3. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보처리내역에 대한 책임 추적성을 확보 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법	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. 3. 동일 계정 동시 사용 시 제한 여부 확인 1) 발급된 계정을 여러 사람이 동시에 사용하지 못하게 시스템상에서 제한하고 있는지 확인합니다. 
점검 기준	◦ 미조치 : 사용자계정을 다른 개인정보취급자 등과 공유하는 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p264 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p48 이미지 출처: 한국인터넷진흥원, "개인정보 영향평가 수행안내서(2018)", p302

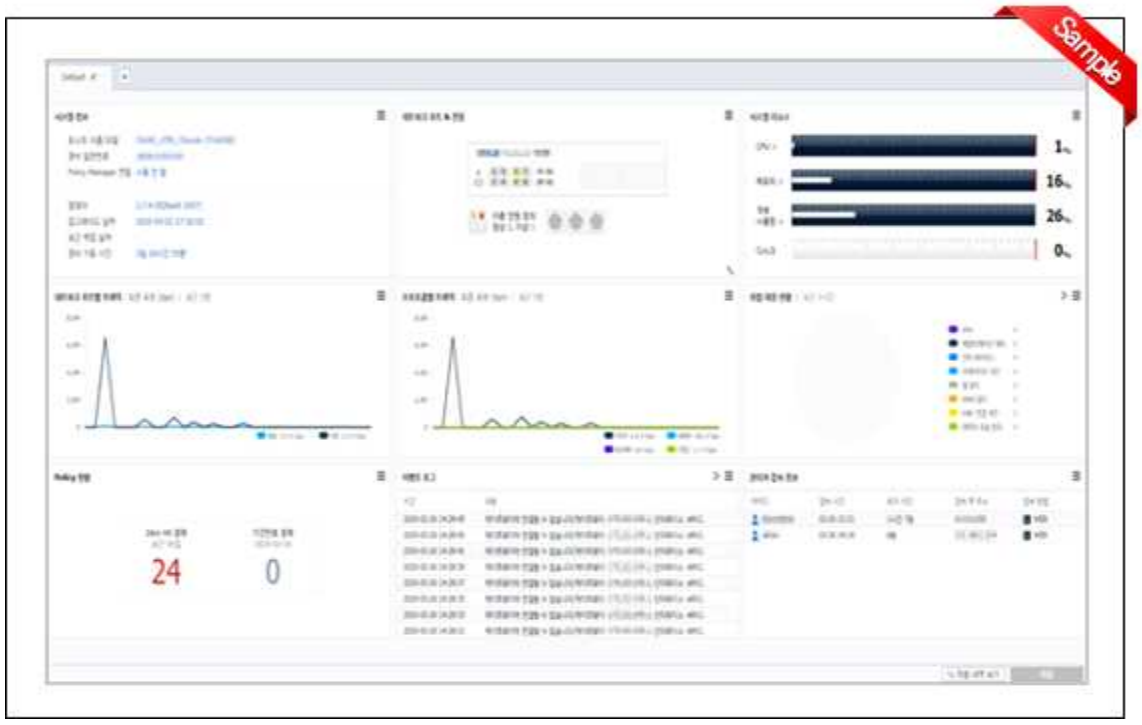
9	개인정보취급자 또는 정보주체가 안전한 비밀번호 작성규칙을 수립하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)** **→ 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립·적용하는지 확인** 1. 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷 홈페이지 등에 적용 2. 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합, 구성 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법	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. 2. 수립된 비밀번호 작성규칙 실제 시스템 적용 확인 1) 관련 지침을 통해 수립한 패스워드 작성규칙을 실제 개인정보처리시스템에 적용·이행하고 있는지 확인합니다. 2) 비밀번호는 8자리 이상 2종류(영문, 숫자, 특수문자) 이상의 문자로 구성하거나 10자리 이상 1종류 문자로 구성합니다. 단, 숫자로만 구성할 경우 취약할 수 있습니다. 
점검 기준	◦ 미조치 : 비밀번호 작성규칙을 수립·적용하지 않는 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p264 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p48~49

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

② 개인정보처리시스템 보유 기관 증빙자료 제출 항목(2/8)

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(공동인증서, OTP 등)을 적용하여 정당한 접근 권한 자임을 확인하는 등의 조치 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법	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 제한하는지를 확인합니다. ※ 개인정보취급자에게 개인정보처리시스템에 대한 접근을 재부여하는 경우에도 반드시 개인정보취급자 여부를 확인 후 계정 잠금 해제 등의 조치가 필요합니다.
점검 기준	◦ 미조치 : 비밀번호 입력 횟수 제한을 하지 않는 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 시스템 로그인 시 비밀번호 일정 횟수 이상 잘못 입력으로 인한 접근 제한 적용 화면 <필수>** 
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p264 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p49~50 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p40

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 IP주소로 제한하는지 여부** 1. 개인정보처리시스템에 대한 접속 권한을 IP주소로 제한하여 인가받지 않은 접근을 제한 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법	1. 개인정보처리시스템 접근통제 확인 1) 운영 중인 개인정보처리시스템에 지정된 IP만 접근할 수 있도록 설정되어 있는지 확인합니다. 2) 단순 ID별, 사용자 그룹별 접근제한이 아닌 IP(Internet protocol)주소, 포트(Port), MAC (Media Access Control) 주소로 제한하도록 합니다.  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 보안 프로그램을 이용하여 접근통제를 실시할 수 있습니다. ※ PC, 노트북 등의 업무용 컴퓨터의 운영체제(OS)에서 제공하는 접근통제 기능 설정 방법 (업무용 컴퓨터 : 제어판 → Windows 방화벽 → Windows 방화벽 설정 또는 해제)
점검 기준	◦ 미조치 : 개인정보처리시스템 접속권한을 IP주소로 제한하지 않은 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p265 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p52

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 제한하는지 여부** 1. 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출시도 탐지 및 대응 ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법	1. 침입차단시스템 및 침입탐지 시스템 확인 1) 침입차단시스템 및 침입방지시스템을 설치하여 운영하고 있는지 확인합니다. 2) 스위치 등의 네트워크 장비에서 제공하는 ACL(Access Control List : 접근제어목록) 등 기능을 이용하여 IP주소 등을 제한함으로써 침입차단 기능을 구현할 수 있습니다. 3) 공개용 소프트웨어를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당 기능을 포함한 시스템을 설치·운영하는지 확인합니다. (다만, 공개용 소프트웨어를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검하고 정기적인 업데이트 여부 등 확인 후 적용 필요) 4) 인터넷데이터센터(IDC), 클라우드 서비스, 보안업체 등에서 제공하는 보안서비스 등도 활용 가능합니다. 5) 불법적인 데이터가 탐지되면 관리자에게 보고 후 대응·조치하도록 합니다. 
점검 기준	◦ 미조치 : 개인정보처리시스템에 접속한 불법적인 개인정보 유출시도에 대응하지 않을 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p265 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p52

13	외부에서 개인정보처리시스템에 접속 시, 가상사설망(VPN), 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하고 있는지 여부

③ 개인정보처리시스템 보유 기관 증빙자료 제출 항목(3/8)

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

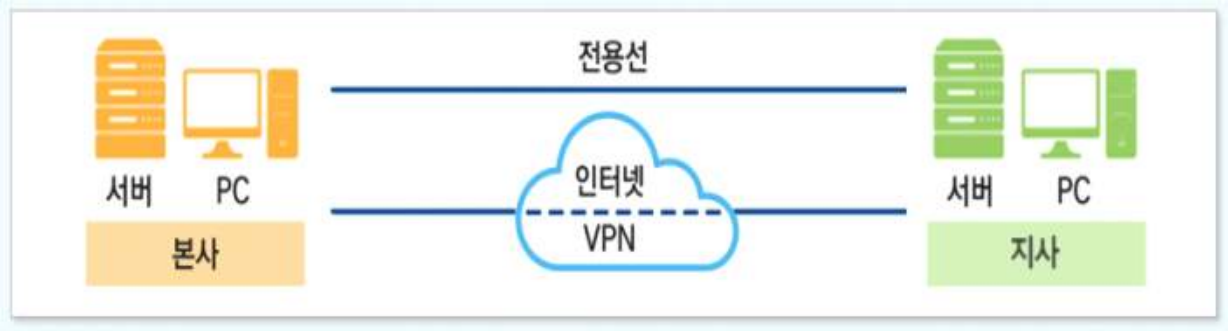
점검 방법

1. 외부에서 접근가능한 개인정보처리시스템 확인

1) 반드시 업무상 외부에서의 접근이 필요한 경우 VPN, 전용선 등 전송구간에 대한 침해사고를 방지할 수 있는 기술적 보안조치를 이행합니다.

※ 외부에서 개인정보처리시스템에 접근 : 출장, 재택근무 등 기관 외 장소에서 개인정보처리시스템에 접근하는 경우

※ 가상사설망(VPN : Virtual Private Network) : 개인정보취급자, 또는 본점과 지점 간 직통으로 연결하는 회선 등을 의미



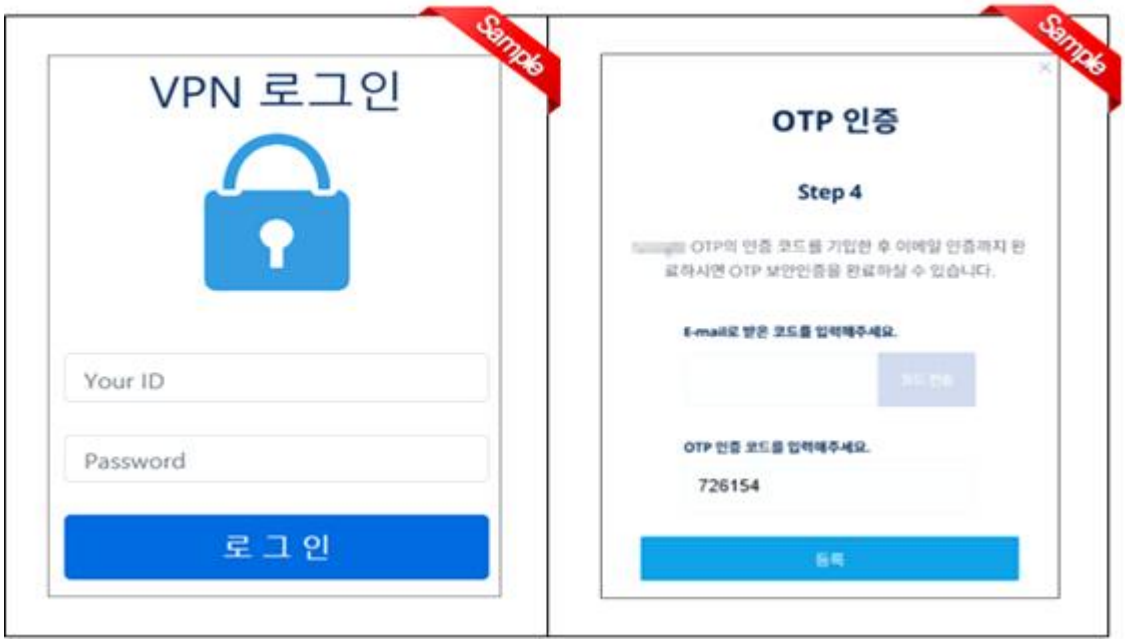
2. 안전한 인증수단 제공 여부 확인

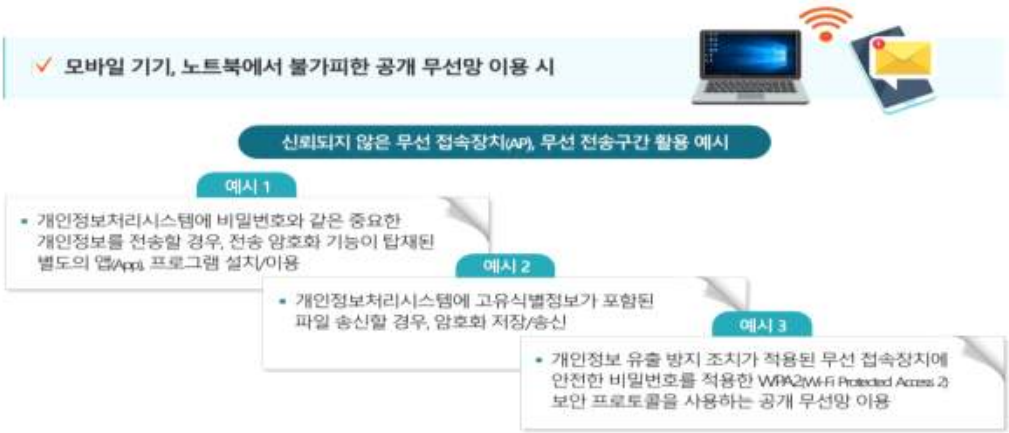
1) 외부에서 내부로 접근할 경우 ID/비밀번호 입력 외에 추가로 PKI, 핸드폰 인증, 이메일 인증 등 추가 인증수단을 통해 접속하는지 확인합니다.

※ 인증서(PKI, Public Key Infrastructure) : 전자상거래 등에서 상대방과의 신원확인, 거래 사실 증명, 문서의 위·변조 여부 검증 등을 위해 사용하는 전자서명으로서 공동인증서 등 해당 전자서명을 생성한 자의 신원을 확인하는 수단

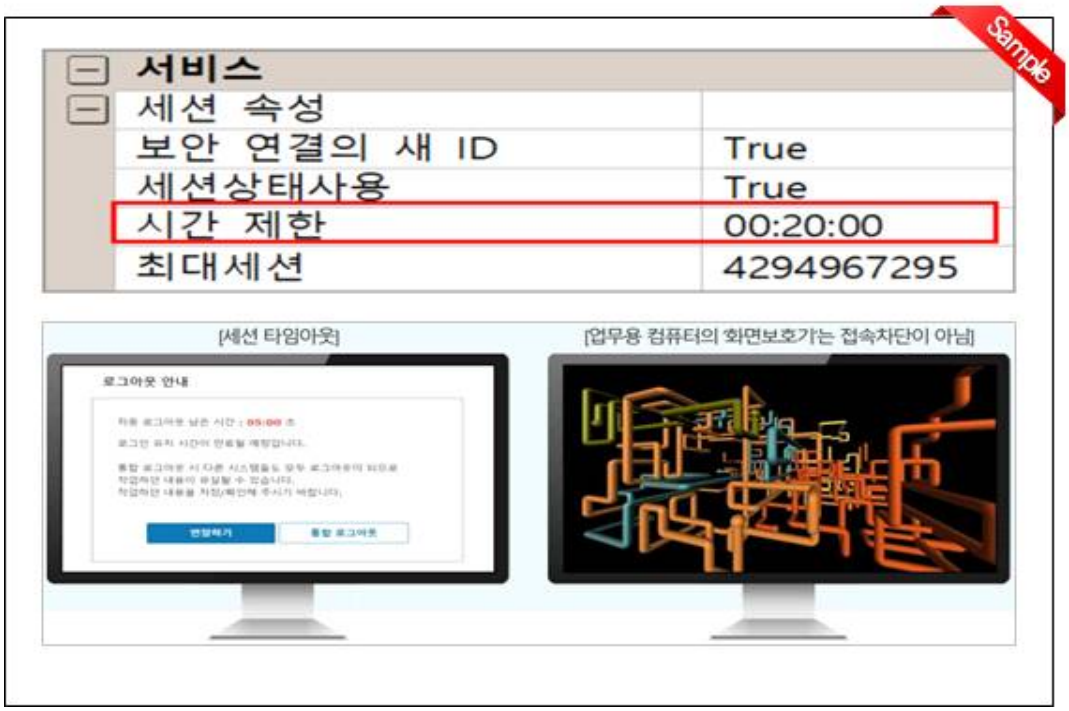
※ 일회용 비밀번호(OTP, One Time Password) : 무작위로 생성되는 일회용 비밀번호



점검 기준	◦ 미조치 : 외부에서 개인정보처리시스템 접속 시 안전한 접속수단 및 인증수단을 적용하지 않는 경우 ◦ 해당없음 : 개인정보처리시스템 미보유하거나 외부에서 접속이 불가한 경우
증빙 자료	**1. 외부에서 시스템 접속 시 VPN, OTP, 핸드폰·이메일·공동인증서 인증 등 안전한 접속수단 또는 인증수단을 적용한 화면 <필수>** 
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p265 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p53~54 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)",p57, p58

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 조치하는지 확인**
점검 방법	1. P2P, 웹하드, 공유설정 등 사용가능 확인 1) 원칙적으로 P2P 사용은 금지됩니다. 망분리를 하지 않은 경우 모든 P2P와 웹하드에 대해 통제를 하기 어려우나 잘 알려진 공유 프로그램에 대해서는 반드시 보안장비의 허용거부 등의 정책 적용이 필요합니다. 2) P2P, 공유설정이 업무상 꼭 필요한 경우라도 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여야 합니다.  2. 공개된 무선망을 이용하여 개인정보 처리하는 경우 유출 차단조치 확인 1) 고유식별정보 송·수신 시 SSL, VPN 등이 적용된 전용 프로그램을 사용하는지 확인합니다. 2) 공개된 무선망 이용 시, 무선접속장치(AP)에 안전한 비밀번호가 적용된 WPA2(Wi-Fi Protected Access 2) 보안 프로토콜을 사용하는지 확인합니다. 
점검 기준	◦ 미조치 : P2P, 공유설정의 사용에 대하여 접근통제를 하지 않는 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p265 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p54~55 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p61, p64

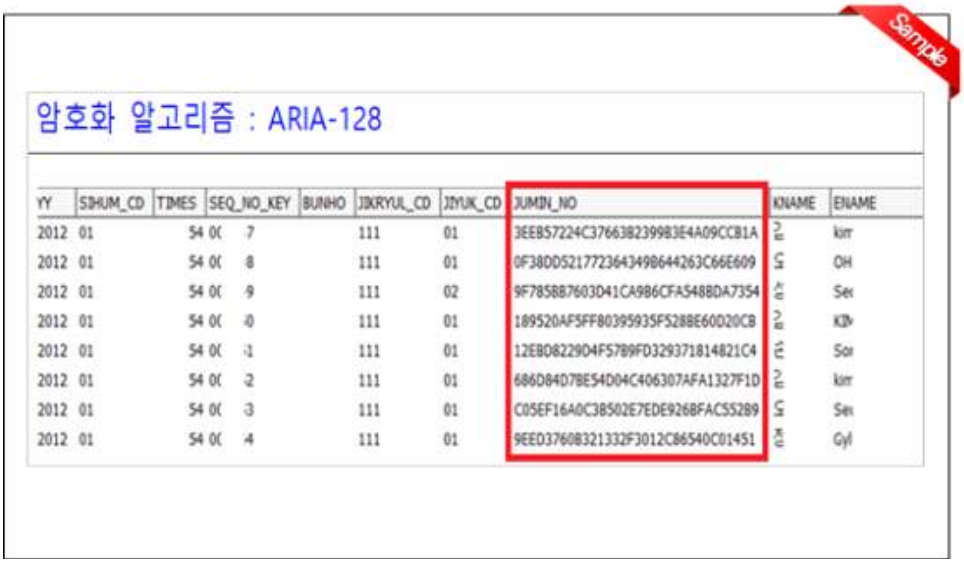
15	인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우, 해당 홈페이지에 대해 연 1회 이상 취약점을 점검 및 그에 따른 개선조치를 하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제6조(접근통제)** **→ 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하는지 여부 확인** ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법	1. 인터넷 홈페이지 내 고유식별정보 처리 여부 확인 1) 홈페이지 내 고유식별정보를 처리한다면 연 1회 취약점 점검을 실시하고, 고유식별정보를 처리하지 않는다면 해당없음 처리합니다. 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 사용합니다. 3. 취약점 점검/개선 조치 참고자료 **취약점 점검/조치 활용 참고 자료 (기술문서)** ▪ 전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드 (행정안전부, 2019.11.) ▪ 공개소프트웨어를 활용한 소프트웨어 개발보안 진단 가이드 (행정자치부, 2016.2.) ▪ 모바일 대민서비스 보안취약점 점검 가이드(행정자치부, 2015.12.) ▪ 홈페이지 취약점 진단·제거 가이드 (KISA, 2013.12.) ▪ 소프트웨어 보안약점 진단가이드 (안전행정부, 2013.11.) ▪ 소프트웨어 개발보안 가이드 (안전행정부, 2013.11.) ▪ 시큐어코딩가이드 (C, Java) (행정안전부, 2012.9.) ▪ Web 2.0 정보보호 실무가이드 (행정안전부, 2010.5.) 
점검 기준	◦ 미조치 : 인터넷 홈페이지에 대하여 연 1회 이상 취약점 점검을 실시하지 않는 경우 ◦ 해당없음 : 인터넷 홈페이지를 통해 고유식별정보를 처리하지 않는 경우
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p265 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p56 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p73

16	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 개인정보처리시스템에 접속을 차단하고 있는지 여부
④ 개인정보처리시스템 보유 기관 증빙자료 제출 항목(4/8)	
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	1. 개인정보처리시스템 내 세션차단 기능 확인 1) 시스템 내 세션 설정 기능이 있는지 확인 후 적절하게 사용 중인지 확인합니다. 2) 세션 시간의 경우 업무에 따라 설정 가능합니다. 다만 세션 시간에 대한 입증책임은 개인정보처리자가 부담합니다. 3) 컴퓨터의 화면보호기의 경우 접속차단으로 볼 수 없습니다.
점검 기준	◦ 미조치 : 일정시간 이상 업무처리를 하지 않을 경우, 개인정보처리시스템에 대한 접속을 차단하지 않는 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 시스템 접속 후 일정시간 이상 시스템 미사용으로 인한 접근 제한 적용 화면 또는 시스템 시간제한 설정 화면 <필수>** 
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p257 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p57 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p74

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 조치하는지 여부**
점검 방법	1. 정보통신망을 통하여 송·수신하는 고유식별정보를 확인합니다. 1) SSL 적용 또는 안전한 암호화 알고리즘을 사용하여 송·수신하는 고유식별정보를 암호화하는지 확인합니다. 2) 시스템이 없는 경우에도 고유식별정보가 포함된 파일을 개인정보 취급자 간 전송한다면 암호화 하는지 확인합니다.(이메일, 메신저 첨부문서 암호화) 2. 보조저장매체를 통하여 전달하는 고유식별정보를 확인합니다. 1) 암호화 기능을 제공하는 보안 USB 등의 보조저장매체를 사용하는지 확인합니다. 2) 해당 개인정보를 암호화하여 저장한 후, 보조저장매체를 사용하는지 확인합니다. ※ 예시 : 고유식별정보가 있는 업무용 파일(Excel 등)을 USB에 저장하여 전달 
점검 기준	◦ 미조치 : 고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우, 암호화 미조치할 경우 ◦ 해당없음 : 고유식별정보를 송신 또는 보조저장매체를 통해 전달하지 않는 경우
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p266~267 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p61~69 행정자치부, 한국인터넷진흥원, "개인정보의 암호화 조치 안내서(2017.1)"

18	내부망에 고유식별정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는지 여부

⑤ 개인정보처리시스템 보유 기관 증빙자료 제출 항목(5/8)

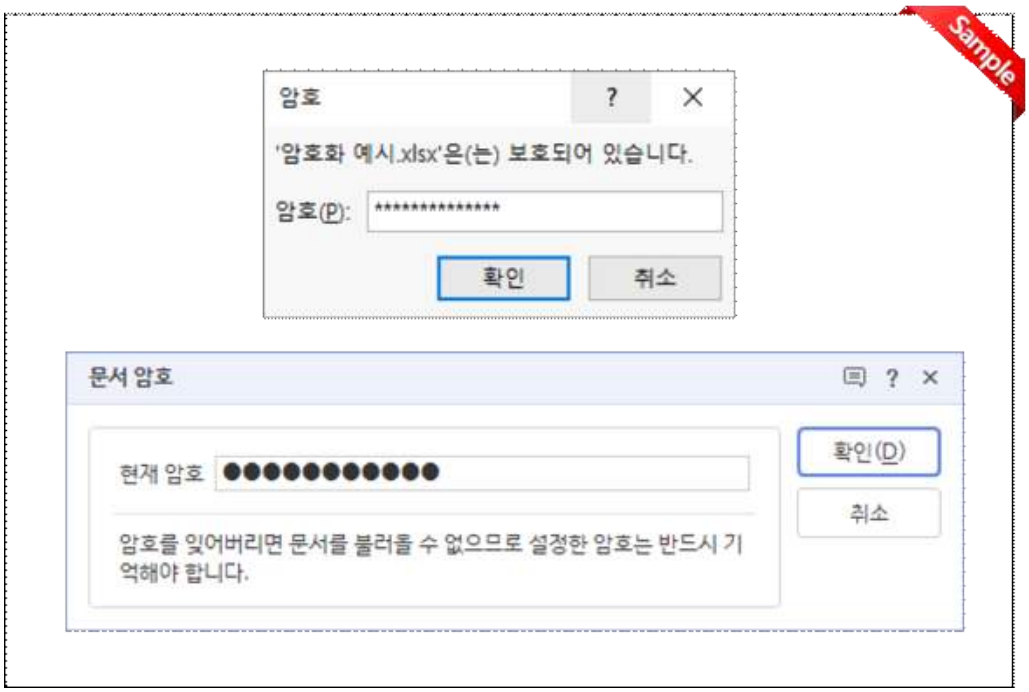
관련 규정	**개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)** **→ 내부망에 고유식별정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는지 여부** ※ 개인정보처리시스템 미보유 시 점검하지 않음
점검 방법	1. 내부망에 고유식별정보 저장 여부 확인 1) 내부망에 저장 중인 고유식별정보가 있는지 확인합니다. 2) 개인정보처리자는 암호화 미적용 시 "위험도 분석"에 따른 결과를 확인합니다 3) 위험도 분석 기준은 내부망에 고유식별정보를 암호화하지 않고 저장하는 경우 개인정보처리자가 이행하여야 할 최소한의 보호조치 기준으로 어느 하나의 항목이라도 '아니오'에 해당한다면 암호화 대상입니다. 2. 고유식별정보 전송 및 보관 시 암호화 여부 확인 1) 내부망에 고유식별정보를 안전한 암호화 알고리즘을 사용하여 암호화를 하고 있는지 확인합니다. ※ 안전한 알고리즘: AES-128/192/256, SEED, HIGHT, ARIA-128/192/256 등 ※ 안전하지 않은 알고리즘: DES, 자체 개발 알고리즘
점검 기준	◦ 미조치 : 내부망에 고유식별정보를 저장하는 경우, 암호화 미조치할 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 시스템 내 고유식별정보가 안전한 알고리즘으로 암호화되어있는 화면 및 알고리즘명 <필수>** 
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p266~267 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p61~69 행정자치부, 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	1. 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립・시행 여부 확인 1) 암호 키와 관련된 절차를 수립하여 시행하고 있는지 확인합니다. 2) 암호 키는 암호화된 데이터를 복호화 할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 매우 중요하며 라이프사이클 단계별 암호 키 관리 절차를 수립 시행하여야 합니다. 3) 암호 키 관리 조치 참고자료 
점검 기준	◦ 미조치 : 암호 키를 안전하게 보관하기 위한 절차를 수립하지 않는 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p266~267 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p67 행정자치부, 한국인터넷진흥원, "개인정보의 암호화 조치 안내서(2017.1)" 미래창조과학부, 한국인터넷진흥원, "암호 키 관리 안내서(2014.12)" 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p85

20	업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하는지 여부

⑥ 개인정보처리시스템 보유 기관 증빙자료 제출 항목(6/8)

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	1. 업무용 컴퓨터 또는 모바일 기기 등에 고유식별정보를 포함한 파일 여부 확인 1) 개인정보처리시스템 또는 업무용 컴퓨터 내에 고유식별정보를 포함한 데이터베이스, 파일 등이 암호화 되어있는지 확인합니다. 2) 업무용 컴퓨터 내 파일 암호화 방법  3) 모바일 기기 내 고유식별정보를 포함한 경우 파일 등이 암호화 되어 있는지 확인합니다. 

점검 기준	◦ 미조치 : 업무용 컴퓨터, 모바일 기기에 저장된 고유식별정보 암호화 미조치할 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 업무용 PC 내 전자문서 암호 입력 화면 또는 암호화 솔루션 적용 화면 <필수>** 
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p266~267 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p68 행정자치부, 한국인터넷진흥원, "개인정보의 암호화 조치 안내서(2017.1)" 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p63, p86

21	개인정보취급자가 개인정보처리시스템에 접속한 기록을 2년 이상 보관·관리하고 있는지 여부
⑦ 개인정보처리시스템 보유 기관 증빙자료 제출 항목(7/8)	
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	1. 개인정보처리시스템 내 접속기록 로그 확인 1) 개인정보처리시스템 내 접속기록 로그를 확인합니다. 2) 접속기록 로그를 2년 이상 관리하고 있는지 확인합니다. 3) 최근 2021년 접속기록 로그보다 이전 2019년 로그를 위주로 확인합니다.
점검 기준	◦ 미조치 : 개인정보처리시스템에 접속한 기록을 2년 이상 보관, 관리하고 있지 않은 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 2년 이상(2019. 5. 이전 날짜)의 개인정보처리시스템 접속기록 로그 <필수>**
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p267 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p70~72 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p90



번호	접속일	접속시간	계정 (ID)	접속지정보 (IP)	수행업무 (이벤트)	정보주체 정보
1	2019-07-06	10:15:10	gdhong01	192.168.4.123	고객정보 조회	A고객카드문의
2	2019-07-06	10:16:05	gjlim02	192.168.4.17	고객정보 수정	B고객주소변경
3	2019-07-06	11:10:47	jskim01	192.168.4.34	직원 조회	부서발령통지

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
점검 방법	1. 개인정보처리시스템 내 접속기록 로그 확인 1) 개인정보처리시스템 내 접속기록 로그를 확인합니다. 2) 접속기록 로그에 5가지 필수사항이 모두 포함되어 있는지 확인합니다. (계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무) 
점검 기준	◦ 미조치 : 개인정보처리시스템에 접속한 기록에 5가지 필수항목이 없는 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p267 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p70~72 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p90

23	악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영 및 최신의 상태로 유지하고 있는지 여부

⑧ 개인정보처리시스템 보유 기관 증빙자료 제출 항목(8/8)

관련 규정

개인정보의 안전성 확보조치 기준 제9조(악성프로그램 등 방지)
→ 악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하고 최신의 상태로 유지하는지 여부

1. 보안 프로그램의 자동업데이트 기능을 사용하거나, 일 1회 이상 업데이트하여 최신의 상태로 유지
2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

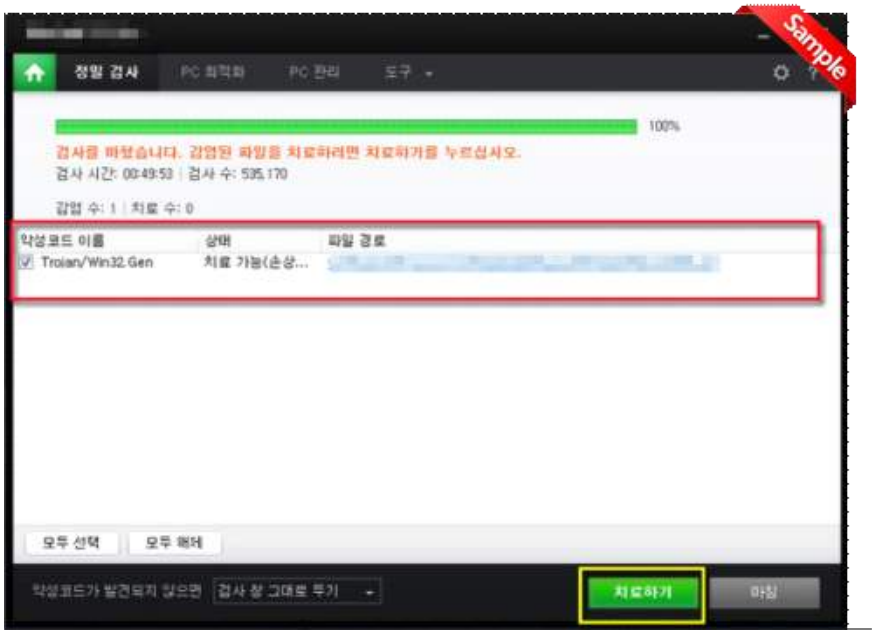
점검 방법

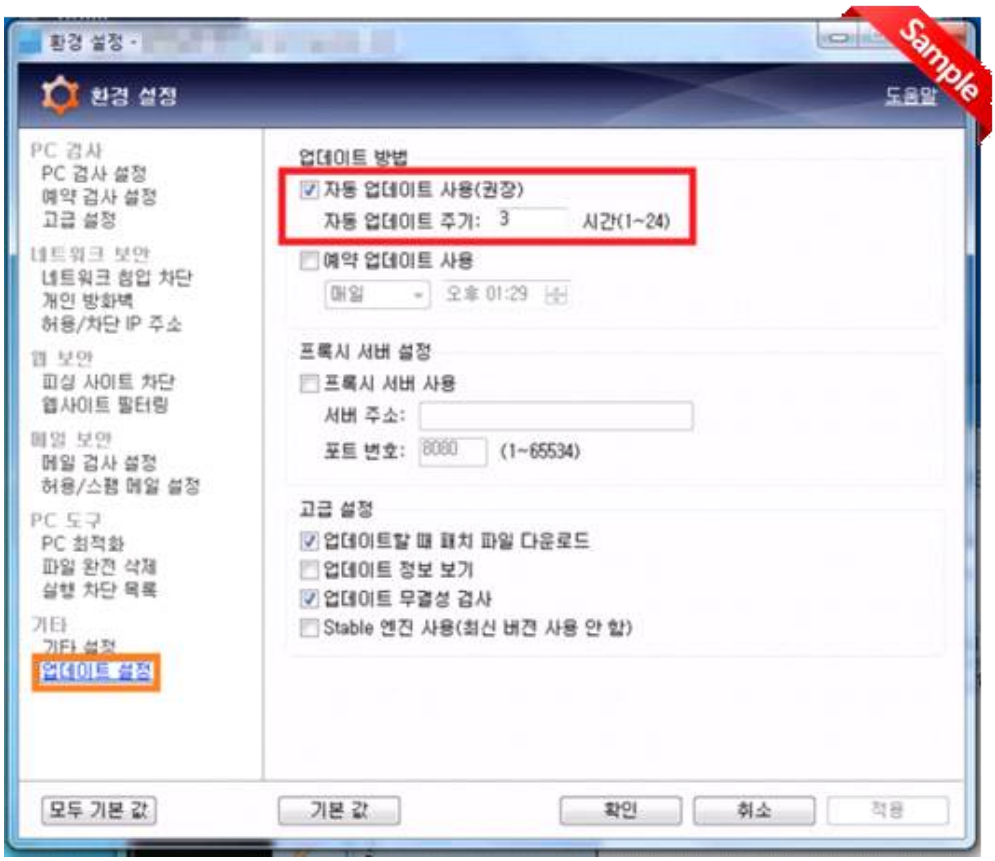
1. 보안 프로그램 설치·운영
   1) 단말기 내 보안 프로그램 설치 여부를 확인합니다.
   2) 보안 프로그램이 항상 실행되어 있는지 여부를 확인합니다.

2. 보안 프로그램 최신 업데이트
   1) 일 1회 이상 업데이트를 하는지 여부를 확인합니다.

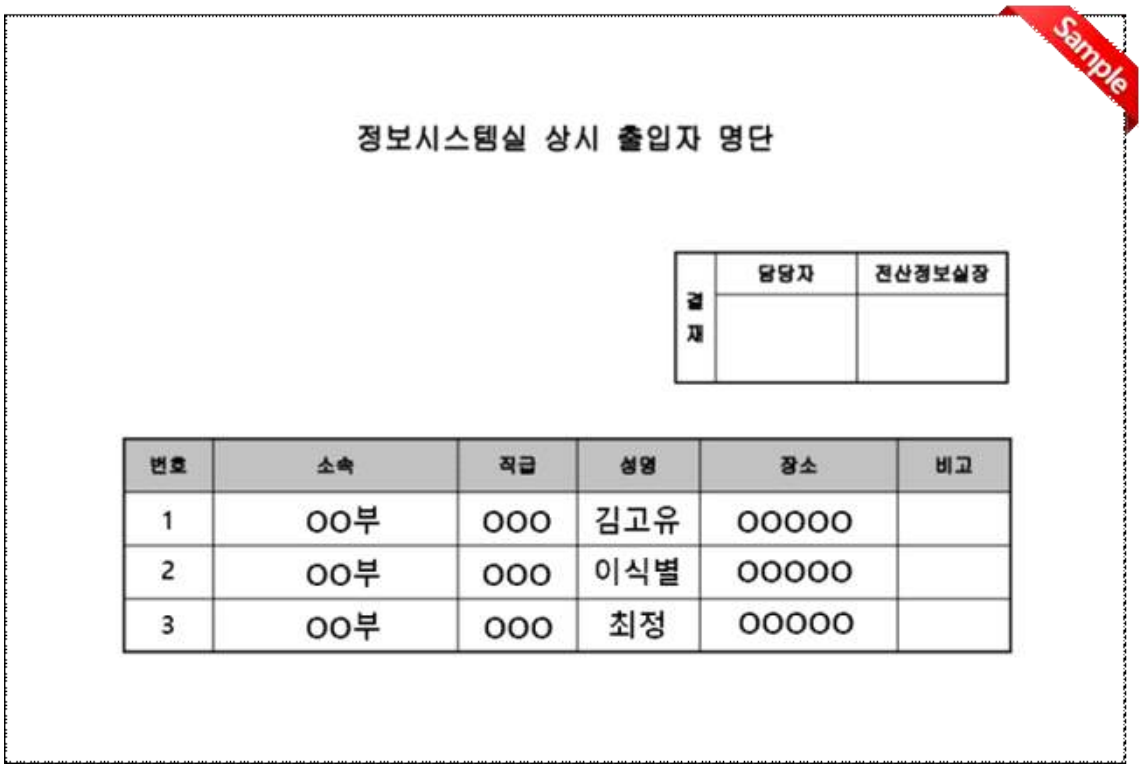


3. 발견된 악성프로그램에 대한 대응 조치
   1) 보안 프로그램을 통해 발견된 악성프로그램 등에 대하여 삭제, 치료 등의 대응 조치를 하는지 확인합니다.



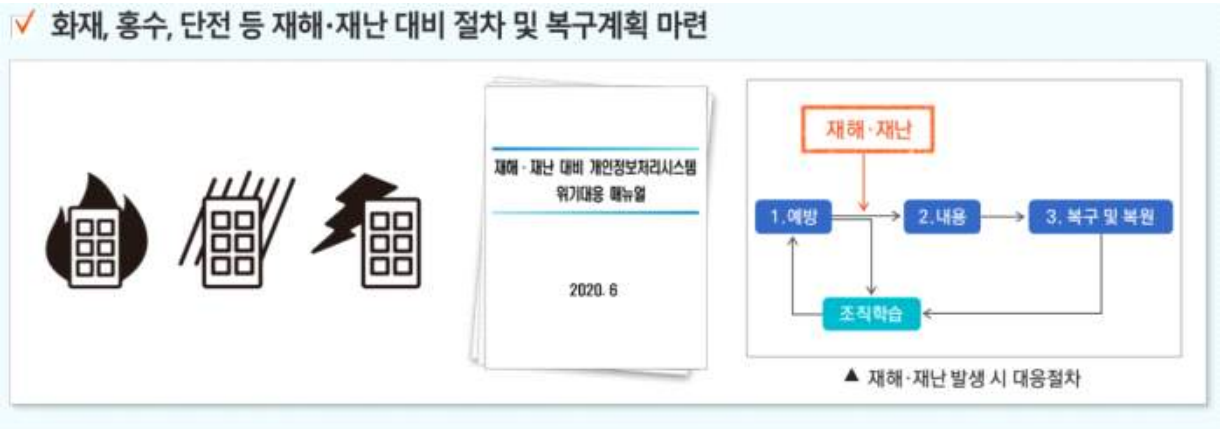
점검 기준	◦ 미조치 : 백신프로그램을 설치하지 않거나, 최신의 상태로 업데이트를 하지 않는 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 보안 프로그램 자동 업데이트 설정 화면 <필수>** 
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p268 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p75~76

<table>
<tr><td>24</td><td>개인정보처리시스템에 직접 접속하는 관리용 단말기에 대해 비인가자가 임의로 조작하지 못하도록 조치하고 있는지 여부</td></tr>
<tr><td>관련 규정</td><td>개인정보의 안전성 확보조치 기준 제10조(관리용 단말기의 안전조치)
→ 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대하여 안전조치하는지 여부
1. 인가받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 악성프로그램 감염방지 등을 위한 보안 조치 적용
※ 개인정보처리시스템 미보유 시 점검하지 않음</td></tr>
<tr><td>점검 방법</td><td>1. 관리용 단말기 현황 관리(IP주소, 용도, 담당자, 설치 위치 등)
1) 관리용 단말기 위치(전산실)와 담당자 확인합니다.
※ 관리용 단말기: 개인정보처리시스템에 대하여 직접 접속하여 해당 시스템을 개발·운영·관리하는 기기

2. 관리용 단말기 보안
1) 관리용 단말기에 비인가자가 접근하지 못하도록 전산실 출입통제 절차를 수립하고 운영합니다.


2) 관리용 단말기 계정/패스워드, 주요 정보를 전산 담당자가 아닌 다른 사람에게 공유하고 있지 않은지 확인합니다.
3) 관리용 단말기 내 백신검사 등의 감염방지 조치를 정기적으로 실시합니다.</td></tr>
<tr><td>점검 기준</td><td>◦ 미조치 : 관리용 단말기에 대해 안전조치를 하지 않는 경우
◦ 해당없음 : 없음</td></tr>
<tr><td>참고 자료</td><td>개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p268
개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p77~78</td></tr>
</table>

25	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 장소에 보관하고 있는지 여부
② 개인정보처리시스템 미 보유 기관 증빙자료 제출 항목(2/2)	
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 캐비닛 등 안전한 장소에 보관
점검 방법	1. 개인정보의 안전한 보관 여부 확인 1) 개인정보가 포함된 서류, 보조저장매체 등이 자물쇠 등 잠금장치가 있는 캐비닛, 전산실, 자료보관실 등에 보관되고 있는지 여부를 확인합니다. 2) 개인정보가 포함된 서류를 캐비닛에 보관하는 경우, 파기 기한이 경과한 개인정보는 별도로 분리하여 보관합니다.
점검 기준	◦ 미조치 : 개인정보가 포함된 서류, 보조저장매체 등에 대하여 물리적 안전조치를 하지 않을 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 캐비닛, 전산실, 자료보관실 등이 잠금장치가 되어있는 사진 <필수>** 
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p269 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", 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	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. 2. 위기대응 절차 훈련 및 정기적 점검 1) 수립된 대응절차에 대하여 모의 훈련(백업, 복구 등)을 진행하고 정기적으로 점검하여 대응절차에 변경이 있는 경우 변경사항을 반영하는 등의 적절한 조치를 해야 합니다. 
점검 기준	◦ 미조치 : 재해·재난 발생 시, 위기대응 매뉴얼 등 대응 절차를 마련하지 않을 경우 ◦ 해당없음 : 없음
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p269 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p81~83 이미지 출처: 한국인터넷진흥원, "개인정보의 안전성확보조치 기준 교육자료(2020.8.)", p120