2021년 고유식별정보 안전조치 관리실태 조사 매뉴얼(공공-학교)

2021년 4월

개인정보보호위원회
KISA 한국인터넷진흥원

목 차

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 종합지원시스템을 통해 기관 및 담당자정보, 고유식별정보 보유현황 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. 5만 명 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 공공분야 관리실태 **조사 대상은 「초·중등교육법」에 따라 설치된 각 급 학교 (초·중·고등학교 및 기타 학교 등)**입니다.

개인정보보호 종합지원시스템(intra.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, 미 조치 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.

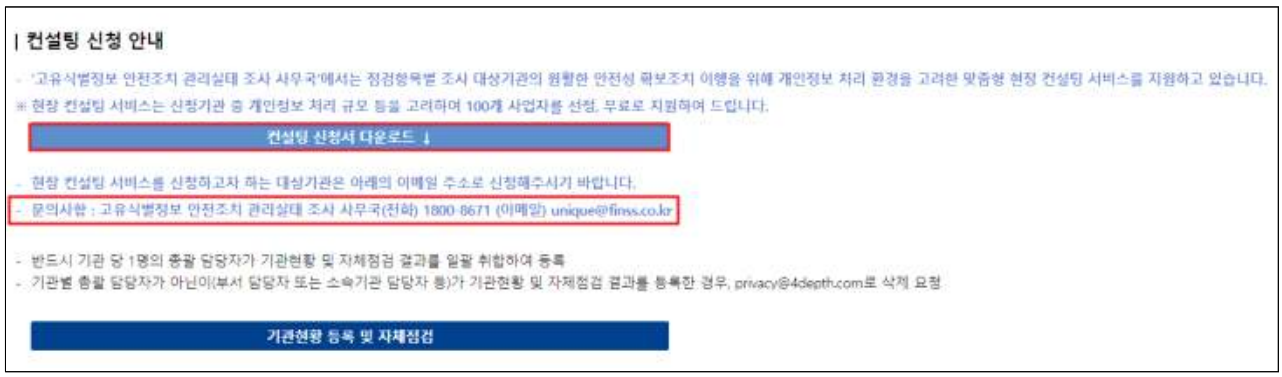
5. 자체점검 진행 시 참고자료 목록

- **고유식별정보 안전조치 관리실태 조사 안내 동영상 등 매뉴얼**
  (종합지원시스템 → 고유식별정보 실태조사 → 기관현황등록 자체점검) 또는
  (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 내려 받아 신청서를 작성한 뒤, 하단의 고유식별정보 사무국 이메일 주소 (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 종합지원시스템(intra.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?**
공공기관의 경우 보유량과 무관하게 모두 점검대상이며, 초·중등교육법에 따른 각 급 학교는 공공기관에 속하기 때문에 보유량 5만 건이 넘지 않은 경우에도 조사대상입니다.	

Q4	**분교도 따로 등록해야 하나요?**
본교에서 분교에 대한 점검을 진행한 후 본교에서 통합하여 등록합니다.	

Q5	**중학교와 고등학교의 개인정보보호 책임자가 같은데 중학교와 고등학교를 모두 등록해야 하는 건가요?**
중학교와 고등학교의 개인정보보호 책임자를 별도로 등록합니다.	

Q6	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, 공공기관의 경우 10만 명 미만일 경우 유형2, 10만 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]

Q7	개인정보보호 책임자, 개인정보보호 담당자, 개인정보취급자 등록은 어떻게 하나요?

개인정보보호 책임자*는 교장 선생님입니다. 개인정보보호 담당자는 개인정보 처리방침에 공개한 담당자이며, 개인정보취급자는 학교에서 처리하는 개인정보를 처리하는 모든 교직원으로 등록하시면 됩니다.

*개인정보보호 책임자의 경우, 국가법령센터의 교육부 개인정보보호지침에 교장 선생님으로 명시되어 있음

Q8	개인정보취급자 수에 수업만 담당하는 강사도 포함되나요?

개인정보취급자는 개인정보를 조회할 수 있는 모든 관계자이므로 방과 후 강사, 기간제 교사 등 수업만 담당하더라도 학생 정보에 접근 가능하다면 개인정보취급자입니다.

Q9	개인정보취급자 수에 사회복무요원, 조리원, 영양사도 포함되나요?

개인정보취급자는 개인정보를 조회할 수 있는 모든 관계자가 포함되므로, 영양사, 사회복무요원, 조리원이 학생의 개인정보에 접근 가능하다면 취급자로 처리합니다.

Q10	**나이스 시스템, K-에듀파인 시스템에 입력되어있는 학생 정보를 포함하여 고유식별정보 보유량을 계산해야 하나요?**
나이스 시스템, K-에듀파인 시스템에 있는 고유식별정보는 각 시·도교육청에서 일괄 처리하므로 각 학교는 업무용 PC, 생활기록부, *기타 문서자료 등 학교 내에서 자체적으로 보유하고 있는 고유식별정보 보유량만 계산하시면 됩니다. 다만, 해당 시스템에서 출력하여 보관 중일 경우에는 고유식별정보 보유현황에 포함하여야 합니다. *기타 문서자료: 기간제 교사 채용 정보, 학교 행사 시 수집 정보 등	

Q11	**학부모, 교직원을 제외하고 학생의 정보만 고유식별정보 보유량으로 계산하면 되나요?**
학생, 학부모, 교직원을 포함하여 기관에서 고유식별정보를 보유하고 있는 모든 인원의 고유식별정보 보유량을 계산합니다. (병설 유치원의 경우 점검 대상 제외)	

Q12	**나이스 시스템에서 학생 정보(재학생 및 졸업생)는 알 수 있지만, 부모님 정보는 확인이 어렵습니다. 부모님 정보를 산정하려면 일일이 학생 정보를 찾아서 부모님 정보를 산정해야 합니다. 이에 대한 방안이 있나요?**
부모님 정보를 산정하기 어려운 경우, 학생 및 부모님 정보를 '학생 정보 * 3 '로 보유량 산정하시면 됩니다.	

Q13	**주민등록번호가 생년월일만 있는 경우, 고유식별정보인가요? 또, 주민등록번호 일부가 마스킹(예: 901122-1******) 등으로 표시되어있는 경우도 고유식별정보인가요?**
최초 수집 시 생년월일만 수집한다면 고유식별정보가 아닙니다. 다만 고유식별정보 수집 이후 암호화, 마스킹 처리로 인하여 원래 데이터로 복원이 가능한 정보일 경우 고유식별정보입니다.	

Q14	**생활기록부, 건강기록부를 모두 보관 중입니다. 보유량 파악은 어떻게 해야 하나요? 시간제 강사 서류의 경우 동일인의 정보를 초본, 범죄경력조회, 졸업증명서 등 여러 곳에 보유하고 있는데, 모두 각각의 건으로 취급하나요?**
생활기록부, 건강기록부의 경우, '인원수 * 2' 로 보유량 산정하도록 합니다. 시간제 강사 서류는 동일인의 정보가 초본, 범죄경력조회, 졸업증명서 등 여러 파일에 들어있을 경우 각각 1건으로 보아 보유량을 산정합니다.	

Q15	**업무용 PC 고유식별정보 보유량 산정은 어떻게 하나요?**
업무용 PC 파일에 포함된 고유식별정보의 경우 파일의 개수가 아닌 파일에 포함된 고유식별정보 보유량을 파악해야 합니다. 만약에 엑셀 replace 함수 등으로 주민등록번호 뒷자리를 치환(예: 901122-1******처리)한 데이터가 있다면 고유식별정보에 포함하여 산정합니다. 산정 방법의 경우 암호화 솔루션을 사용 후 합산하여 기재하거나, 수작업으로 직접 조사하여 고유식별정보 보유량을 산정하도록 합니다.	

Q16	**개인정보처리시스템에 있는 고유식별정보뿐만 아니라 일반 종이 문서, 업무용 파일에 있는 고유식별정보까지 관리실태 조사대상에 포함되는 것으로 알고 있습니다. 그렇다면 범죄수사 자료나 법원의 소송 관련 서류에 포함된 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·종이 문서·업무용 파일 내 위 사항에 해당하는 고유식별정보가 포함되어 있더라도 관리실태 조사에는 해당하지 않습니다.

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

Q17	**2002년 이전 졸업생에 대한 생활기록부를 서고에 보관하고 있는 경우는 누적 졸업생 숫자를 기준으로 기록하면 되나요?**

현재 보유하고 있는 모든 고유식별정보는 입력 대상으로 2002년 이전 생활기록부의 경우에는 졸업생 숫자를 기준으로 보유량을 산정하시면 됩니다.

Q18	**고유식별정보 중 종이 문서 등의 보유 기간이 정리되어있는 사항이 있는지요?**

각 시·도 교육청에서 배포하는 학교 공통 업무 보존 기간표를 참고하시면 됩니다.

Q19	**초등학교와 중학교의 행정실이 통합하여 운영 중인 경우, 고유식별정보 보유량은 어떻게 파악하나요?**

고유식별정보 보유량은 초등학교, 중학교를 분류하여 각각의 보유량을 파악하시면 됩니다.

Q20	**이전에 있던 학교와 통합된 후 이전 학교의 생활기록부도 고유식별정보 보유량에 포함해야 하나요?**

이전에 있던 학교의 고유식별정보를 같이 관리할 경우, 고유식별정보 보유량에 포함하여 계산하시면 됩니다. 그렇지 않을 경우, 통합 이후 보유 중인 고유식별정보 보유량만 파악해 계산하시면 됩니다.

Q21	**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.

Q22	**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.

Q23	**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

Q24	**현장 컨설팅 접수 방법은 어떻게 되나요? 현장 컨설팅을 받게 될 경우, 지속적인 감시 대상이 되거나 행정처분의 대상이 되지는 않나요?**

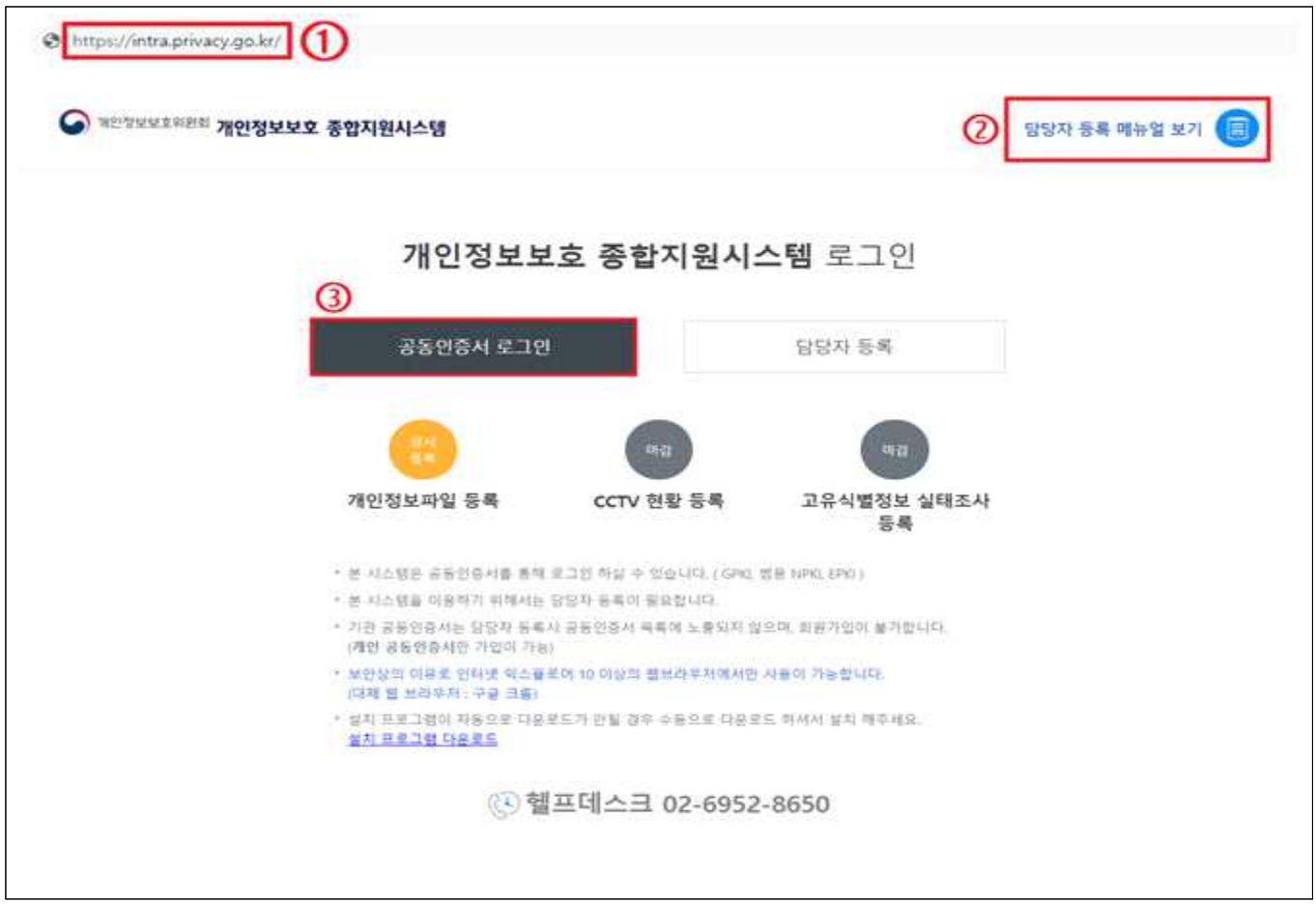
현장 컨설팅은 고유식별정보 관리실태 조사에 관한 상담뿐만 아니라 개인정보보호 관련 전반적인 사항에 관한 상담을 무료로 방문하여 진행하고 있으며, 접수 방법은 개인정보보호 종합지원시스템·개인정보보호 포털 사이트 내에 신청서 양식을 내려받은 후 조사 사무국 이메일로 신청서를 보내주시면 됩니다.
현장 컨설팅은 감사의 목적이 아니라 지원의 목적이기 때문에 컨설팅 이후 지속적인 관리·감시 대상이 된다거나 미비한 사항 적발 시 행정처분을 내리는 등의 불이익은 없습니다.

Q25	**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 및 기관현황 등록 방법



① 개인정보보호 종합지원시스템(https://intra.privacy.go.kr)에 접속합니다.

② 담당자 등록이 되어있지 않은 기관일 경우, 상단의 「담당자 등록 매뉴얼 보기」를 참고해주시기 바랍니다.

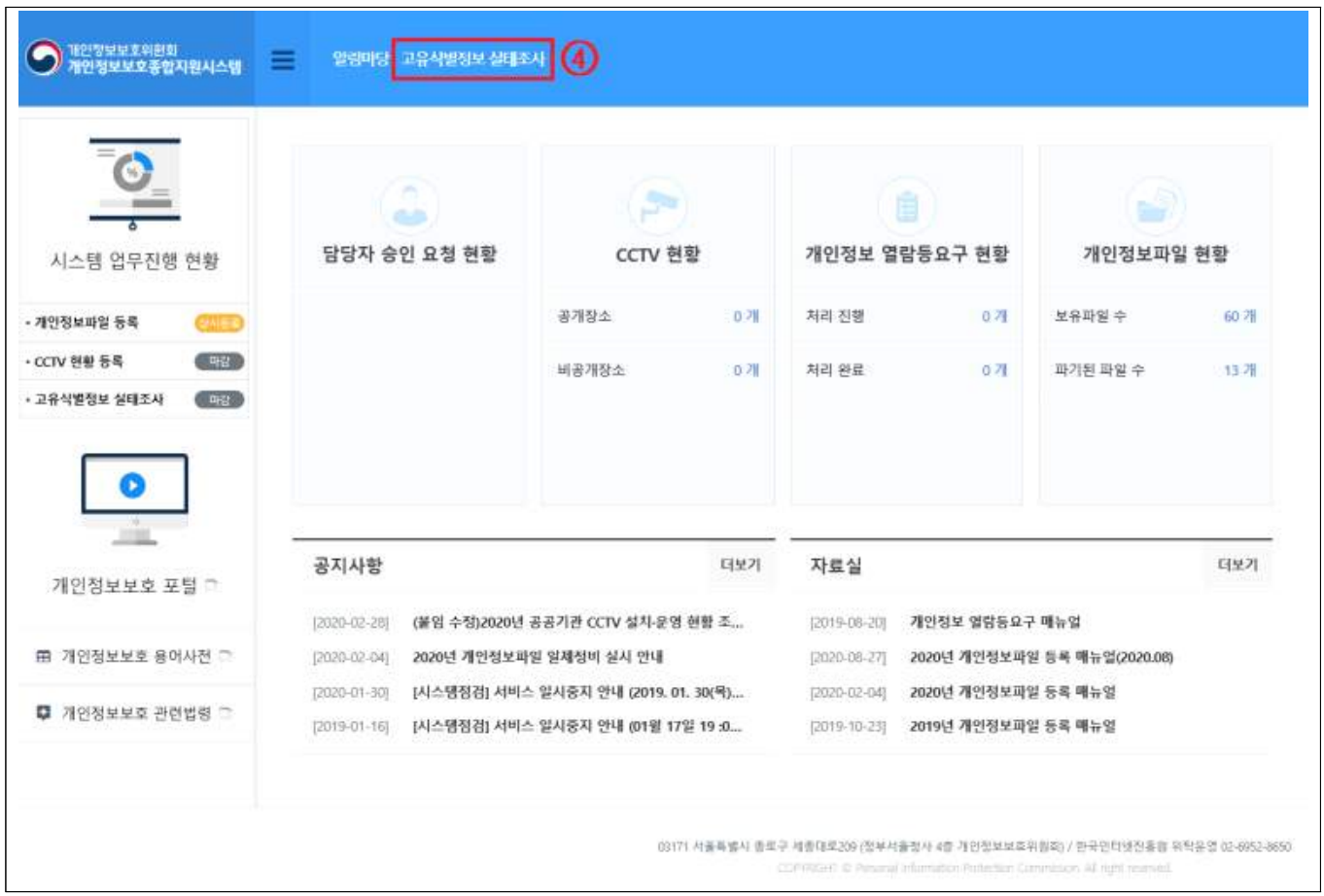
③ 담당자 등록을 마친 기관은 "공동인증서 로그인"을 클릭 후, 사용자 등록 시에 사용했던 공동인증서를 선택하고 비밀번호를 입력합니다.

주의사항

■ 유효기간이 지난 공동인증서로는 로그인 불가

■ 소속기관 변경, 공동인증서 유효기간 만료 등으로 인하여 공동인증서를 재발급받은 경우, 재발급된 공동인증서로 다시 사용자 등록을 하여야 로그인이 가능 (단, 기간 만료 전에 공동인증서를 갱신한 경우에는 계속 사용 가능)

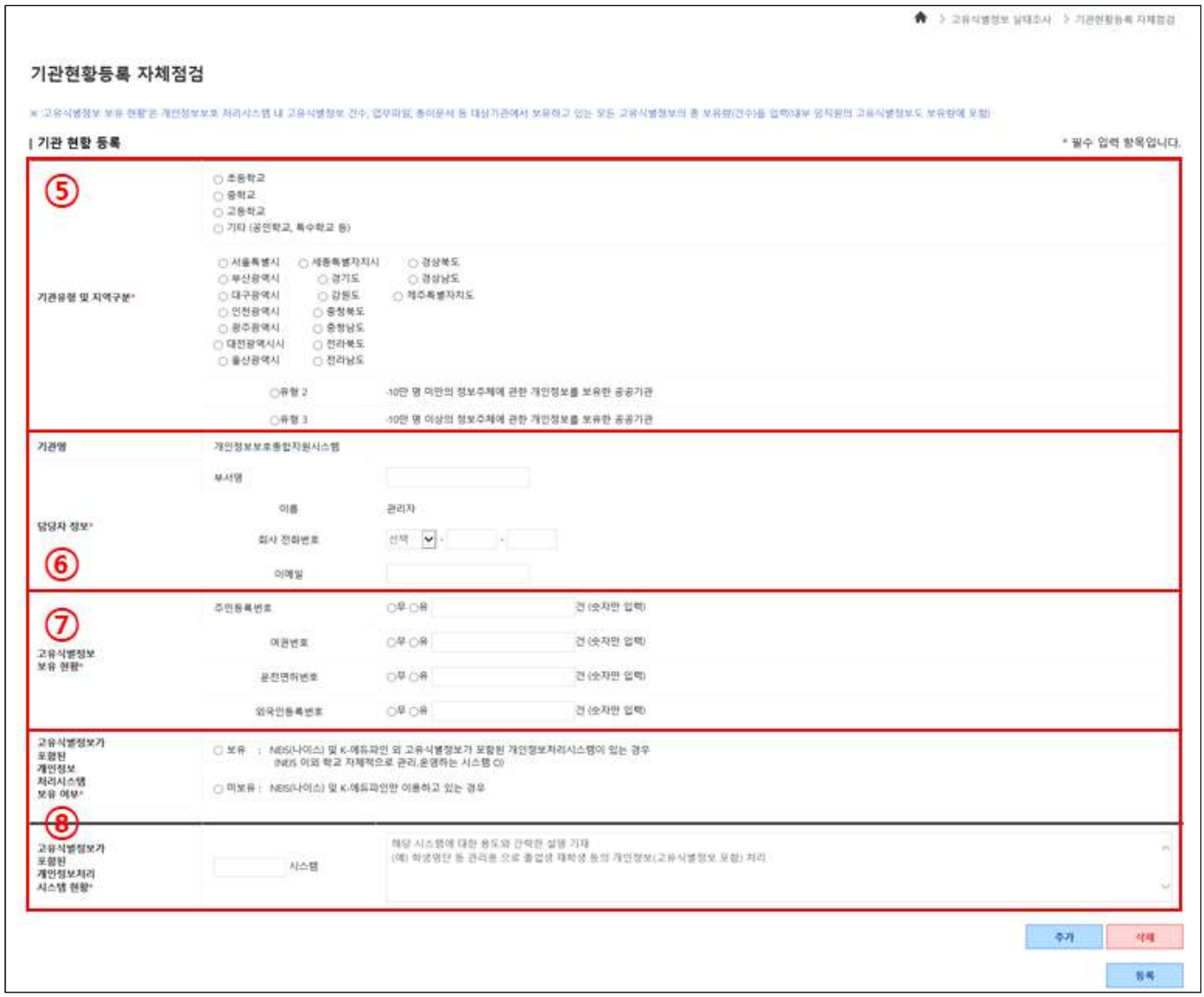
■ 종합지원시스템은 공동인증서를 로그인 용도로만 활용하고 있으며, 공동인증서 비밀번호를 저장하지 않음. 따라서 비밀번호 오류나 변경, 공동인증서 재발급 등 공동인증서 관련 문의는 공동인증서를 발급한 인증기관(행정전자서명 인증관리센터(GPKI), 교육부 행정전자서명인증센터(EPKI) 등)을 통하여 진행



④ 종합지원시스템(https://intra.privacy.go.kr) → 공동인증서 로그인 후, 메인화면의 상단 메뉴 "고유식별정보 실태조사" 버튼 선택 또는 팝업의 바로가기 버튼을 선택합니다.

※ 기관현황 등록사항은 대상기관 담당자 1명이 일괄 등록

※ 보유량과 관계없이 고유식별정보를 처리하는 모든 공공기관은 조사대상에 포함



⑤ 기관 유형 및 지역 구분

: 자신이 속한 기관에 해당하는 분류 및 지역을 하나 선택합니다.

'유형 2' 또는 '유형 3' 중에서 해당하는 유형을 선택합니다.

참고사항

■ 유형 2, 유형 3에서의 개인정보 보유량은 고유식별정보를 포함하여 대상기관이 보유하고 있는 정보주체의 개인정보 보유량을 의미하는 것으로, 10만 이상, 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

⑥ 기관명 및 담당자 정보

: 기관명(학교명) 및 담당자 정보(부서명, 이름, 회사 전화번호, 이메일주소), 기관 내 개인정보취급자 수에 대해 입력합니다.

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

⑦ 고유식별정보 보유현황

: 대상기관에서 현재 보유하고 있는 고유식별정보의 종류와 건수를 입력합니다.

※ 고유식별정보 보유 건수는 교직원, 학부모, 학생의 정보를 모두 포함하여 산정

※ 공공기관이 범죄수사, 재판업무 수행 등 목적으로 처리하는 고유식별정보는 제외
(고유식별정보 안전조치 관리실태 조사 매뉴얼 10p – 관리실태 조사 관련 FAQ 참조)

⑧ 고유식별정보가 포함된 개인정보처리시스템 보유여부 및 현황

: NEIS(나이스) 및 K-에듀파인 외 고유식별정보가 포함된 개인정보처리시스템이 있는 경우에는 보유를, NEIS(나이스) 및 K-에듀파인만 이용하고 있는 경우 미보유를 선택합니다.

고유식별정보가 포함된 개인정보처리 시스템 현황은 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

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.**

4-2 자체점검 제출 방법


고유식별정보 안전조치 자체점검 등록

| 고유식별정보 안전조치 자체점검

NO	세부 점검내용	조치 (있음)	미조치 (없음)	해당 없음	설명
1	수집목적이 달성되었고, 보존기간이 경과한 고유식별정보를 파기하고 있는지 여부	○	○	○	
2	개인정보의 안전한 처리를 위한 내부 관리계획을 수립,시행하고 있는지 여부	○	○	○	
3	개인정보취급자 대상 개인정보보호 교육을 정기적으로 시행하고 있는지 여부	○	○	○	
4	개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고, 전보·퇴직 등 개인정보취급자 변경 시 접근권한을 지체 없이 변경 말소하고 있는지 여부	○	○	○	
5	개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지 않는지 여부	○	○	○	
6	개인정보가 인터넷 홈페이지, P2P, 공유설정 등으로 유·노출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 등에 접근통제 등에 관한 조치를 하고 있는지 여부	○	○	○	
7	고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는지 여부	○	○	○	
8	업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우, 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하는지 여부	○	○	○	
9	악성프로그램을 방지,치유할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치,운영 및 최신의 상태로 유지하고 있는지 여부	○	○	○	
10	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 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 설명을 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

4-3 증빙자료 제출 방법

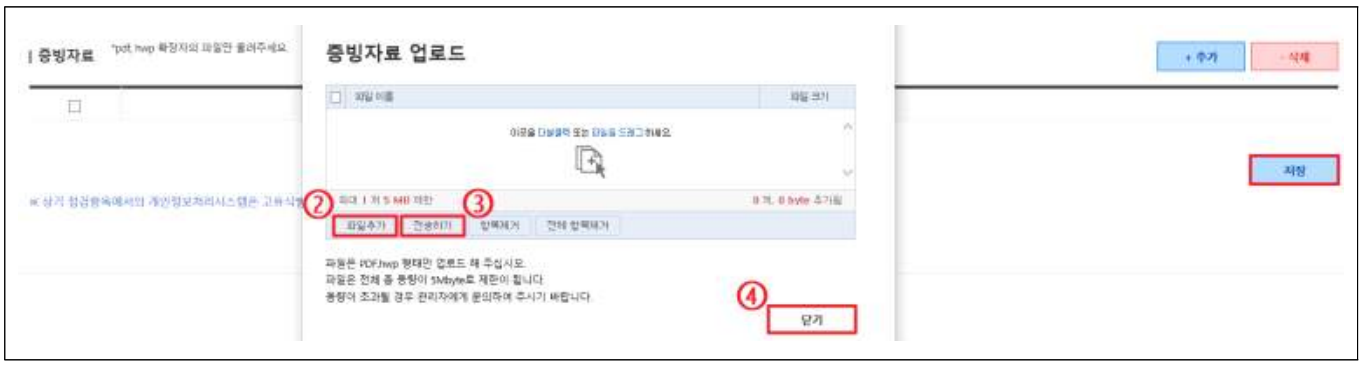
※ 증빙자료 중 4번, 5번 항목은 나이스 시스템, K-에듀파인 시스템을 기준으로 증빙자료를 제출. 권한부여의 경우 시·도교육청이 아닌 학교에서 부여하므로 점검해야 함.

- 4번 항목: 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고, 전보.퇴직 등 개인정보취급자 변경 시 접근권한을 지체 없이 변경.말소하고 있는지 여부
- 5번 항목: 개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지 않는지 여부

※ 고유식별정보 안내 페이지에서 '증빙자료 제출 양식'을 미리 내려 받아 작성

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

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



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

※ 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 [저장] 버튼을 클릭하면 조사가 마무리됩니다.

4-4 수정 방법

❑ 담당자 정보 수정 방법

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

❑ 기관현황 등록 수정 방법

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

① 개인정보보호 종합지원시스템 접속 → 공동인증서 로그인 → 고유식별정보 실태조사 메뉴 선택 → 기관현황 자체점검 메뉴를 선택하면, 등록된 기관현황 정보 및 자체점검 결과를 수정 가능합니다.

❑ 자체점검 수정 방법

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

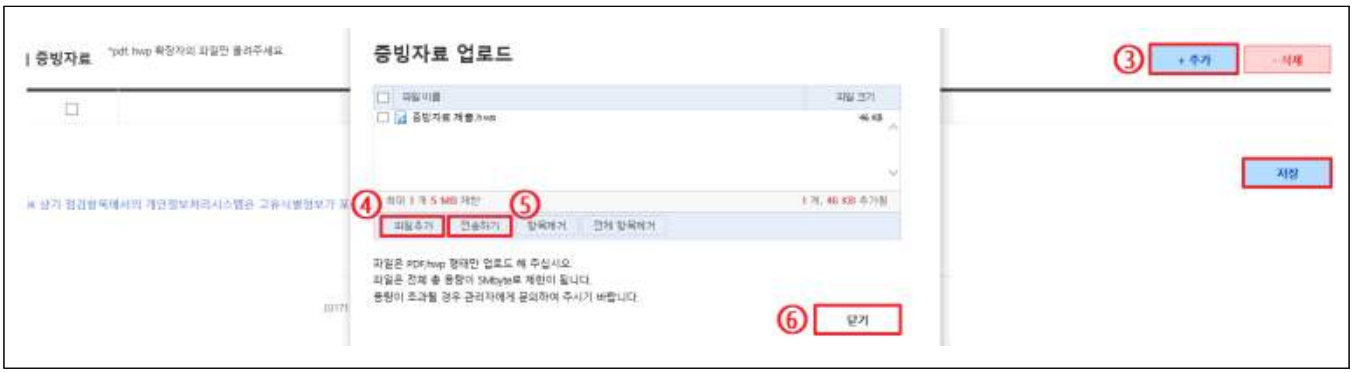
② 기존에 입력한 자체점검 결과에 대하여 수정을 진행합니다.

③ 자체점검 결과의 수정이 완료되면, 페이지 하단의 [저장] 버튼을 클릭하여 조사를 마무리합니다.

❑ 증빙자료 수정 방법

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

② 증빙자료 수정을 위하여 하단의 '증빙자료'를 확인 후, 수정을 원하는 파일에 대해 [-삭제] 버튼을 클릭하여 삭제합니다.



③ 기존에 제출했던 증빙자료의 삭제가 확인되면, 좌측의 [+추가] 버튼을 클릭합니다.

④ '증빙자료 업로드' 팝업화면이 나타나면, '증빙자료 업로드' 항목에 있는 [파일추가] 버튼을 눌러 증빙자료를 시스템에 업로드 합니다.
※ PDF(.pdf), 한글(.hwp) 문서만 등록 가능

⑤ [전송하기]를 눌러 파일을 업로드하면, 증빙자료 제출이 완료됩니다.

⑥ [닫기]를 누르고 나와, 페이지 하단의 [저장] 버튼을 클릭하여 수정을 마무리합니다.

5 점검방법

5-1 자체점검 점검항목

※ 나이스 시스템, K-에듀파인 시스템에 있는 고유식별정보를 제외한 업무용 PC 내 파일에 있는 고유식별정보, 생활기록부 등 종이문서에 있는 고유식별정보만 점검

①	수집목적이 달성되었고, 보존기간이 경과한 고유식별정보를 파기하고 있는지 여부
②	개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행하고 있는지 여부
③	개인정보취급자 대상 개인정보보호 교육을 정기적으로 시행하고 있는지 여부
④	개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고, 전보·퇴직 등 개인정보취급자 변경 시 접근권한을 지체 없이 변경·말소하고 있는지 여부
⑤	개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지 않는지 여부
⑥	개인정보가 인터넷 홈페이지, P2P, 공유설정 등으로 유·노출되지 않도록 개인정보처리시스템, 업무용컴퓨터 등에 접근통제 등에 관한 조치를 하고 있는지 여부
⑦	고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는지 여부
⑧	업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하는지 여부
⑨	악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영 및 최신의 상태로 유지하고 있는지 여부
⑩	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 장소에 보관하고 있는지 여부

5-2 증빙자료 제출 점검항목

※ 증빙자료 중 4번, 5번 항목은 나이스 시스템, K-에듀파인 시스템을 기준으로 증빙자료를 제출. 권한부여의 경우 시·도교육청이 아닌 학교에서 부여하므로 점검해야 함

③	개인정보취급자 대상 개인정보보호 교육을 정기적으로 시행하고 있는지 여부
④	개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고, 전보·퇴직 등 개인정보취급자 변경 시 접근권한을 지체 없이 변경·말소하고 있는지 여부
⑤	개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지 않는지 여부
⑨	악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영 및 최신의 상태로 유지하고 있는지 여부

5-3 점검항목 세부안내

1	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 지체 없이 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 지체 없이 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

2	개인정보의 안전한 처리를 위한 내부관리계획을 수립·시행하고 있는지 여부
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
참고 자료	개인정보보호위원회, 한국인터넷진흥원, “개인정보의 안전성 확보조치 기준 해설서(2020.12)”, p33~45

3	개인정보취급자 대상 개인정보보호 교육을 정기적으로 시행하고 있는지 여부

① 증빙자료 제출 항목(1/4)

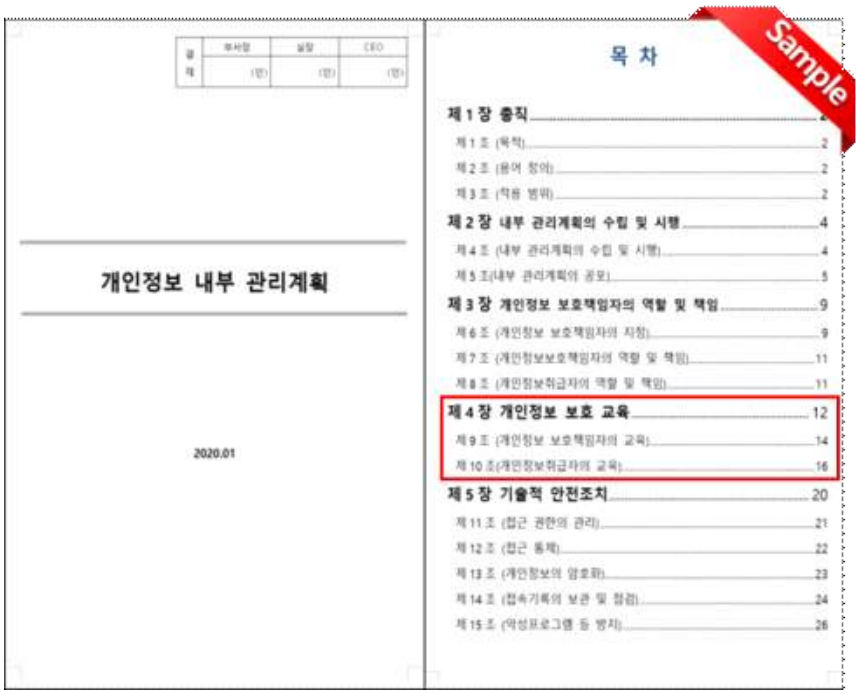
관련 규정	**개인정보보호법 제28조(개인정보취급자에 대한 감독)** **→ 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 시행하는지 여부 확인**
점검 방법	1. 학교 내 정기적인 개인정보보호 교육을 시행하는지 여부 확인 1) 정기적으로 개인정보 교육을 시행하는지 확인합니다. 2. 개인정보보호 교육 내용의 문서화 여부 확인 1) 교육 내용은 반드시 문서화하여 결재를 받은 후 보관합니다. 2) 교육 문서에는 교육자료, 참석자 명단, 교육 사진 등의 내용을 포함합니다.

개인정보보호 교육 참석자 명단

Sample

연 번	부 서	직 급	성 명	서 명
1	○○부	○○○	홍 길 동	
2	○○부	○○○	왕 서 방	
3	○○○부	○○○	아 무 개	
4	○○부	○○○	김 철 수	

3) 위 내용은 내부관리계획 수립 시 반영하여 개인정보 보호책임자는 연 1회 변경사항을 관리합니다.



개인정보 내부 관리계획

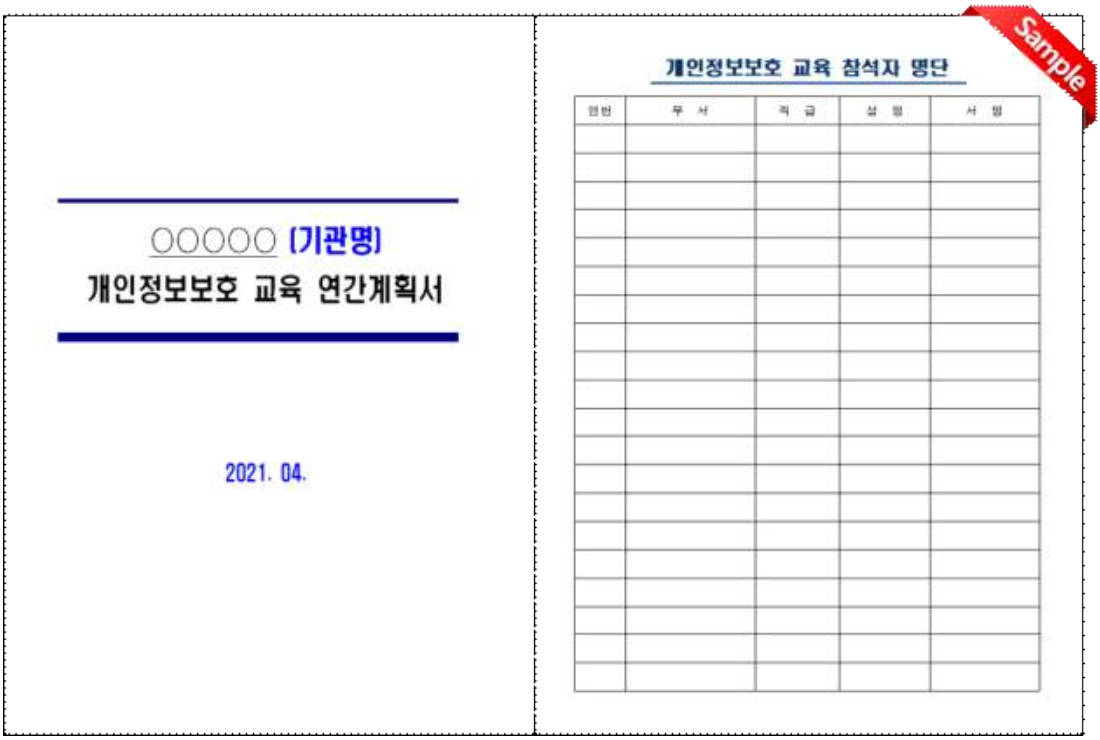
2020.01

목 차

Sample

제 1 장 총칙 1
제 1 조 (목적) 2
제 2 조 (용어 정의) 2
제 3 조 (적용 범위) 2
제 2 장 내부 관리계획의 수립 및 시행 4
제 4 조 (내부 관리계획의 수립 및 시행) 4
제 5 조(내부 관리계획의 공포) 5
제 3 장 개인정보 보호책임자의 역할 및 책임 9
제 6 조 (개인정보 보호책임자의 지정) 9
제 7 조 (개인정보보호책임자의 역할 및 책임) 11
제 8 조 (개인정보취급자의 역할 및 책임) 11
제 4 장 개인정보 보호 교육 12
제 9 조 (개인정보 보호책임자의 교육) 14
제 10 조(개인정보취급자의 교육) 16
제 5 장 기술적 안전조치 20
제 11 조 (접근 권한의 관리) 21
제 12 조 (접근 통제) 22
제 13 조 (개인정보의 암호화) 23
제 14 조 (접속기록의 보관 및 점검) 24
제 15 조 (악성프로그램 등 방지) 26

<내부관리계획 내 개인정보보호 교육>

점검 기준	◦ 미조치 : 정기적으로 개인정보보호 교육을 시행하지 않는 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 개인정보보호 교육 연간계획서 또는 교육 참석자 명단 <필수>** 
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p219

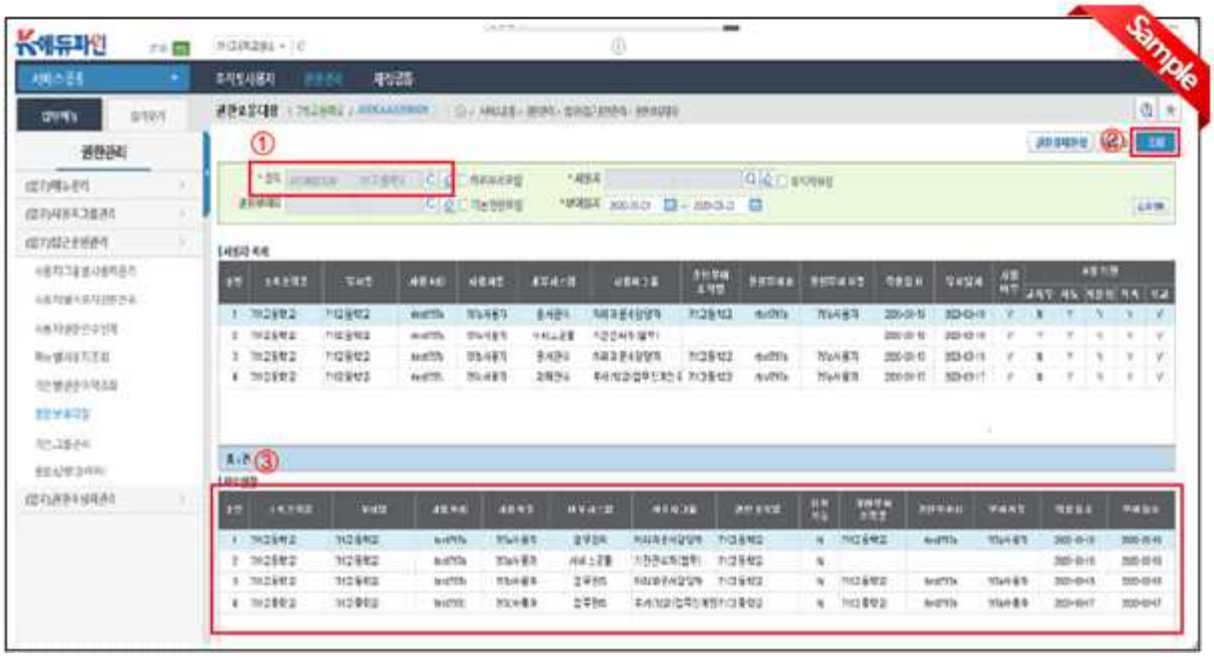
4	개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고, 전보·퇴직 등 개인정보취급자 변경 시 접근권한을 지체 없이 변경·말소하고 있는지 여부

② 증빙자료 제출 항목(2/4)

관련 규정	**개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)** **→ 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고, 전보·퇴직 등 개인정보취급자 변경 시 접근권한을 지체 없이 변경·말소하고 있는지 확인**
점검 방법	1. 기관 내 식별된 개인정보취급자의 담당업무에 적합한 개인정보처리시스템 접근권한 부여 확인 1) 식별된 개인정보취급자의 업무 목적에 적합하게 최소한의 범위로 접근권한이 부여되어 있는지 접근권한 관리 테이블, 접근권한 관리대장 등을 확인합니다. (예) 나이스 시스템: 메뉴 > 시스템관리 > 권한관리 > 사용자권한관리 > 권한보유대장 K-에듀파인: 메뉴 > 서비스공통 > 권한관리 > (업무/재정)접근권한관리 > 권한보유대장 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 관한 확인을 받을 수 있습니다. ※ 접근권한 차등 부여, 개인정보취급자 변경 시 접근권한 변경·말소를 모두 조치하였을 경우 → '조치'로 표시
점검 기준	◦ 미조치 : 접근권한을 차등 부여하고 있지 않거나, 접근권한을 변경·말소 미적용할 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 나이스 시스템, K-에듀파인 등 개인정보처리시스템 접근권한 부여 관리대장 <필수>**

<나이스 시스템 접근권한 부여 관리대장>

증빙 자료



<K-에듀파인 접근권한 부여 관리대장>

Sample

사용자명	사용자ID	시스템	서브시스템	사용자그룹 등록조직	사용자그룹	부여 가능	사용 가능	사용 여부	적용일자	부여일자	부여
OOO	000001	중등 관리	시스템 관리	공통	교육비 지원		O	O	21. 3. 23.	21. 3. 23.	OOO

<서면 접근권한 부여 관리대장>

2. 나이스 시스템, K-에듀파인 등 개인정보처리시스템 접근권한 변경·말소 관리대장 <필수>

Sample

인사이동 및 퇴직 점검표

순번	날짜	사용자	계정	인사이동/퇴직	처리자
1	21. 3. 23.	OOO	000001	퇴직	OOO

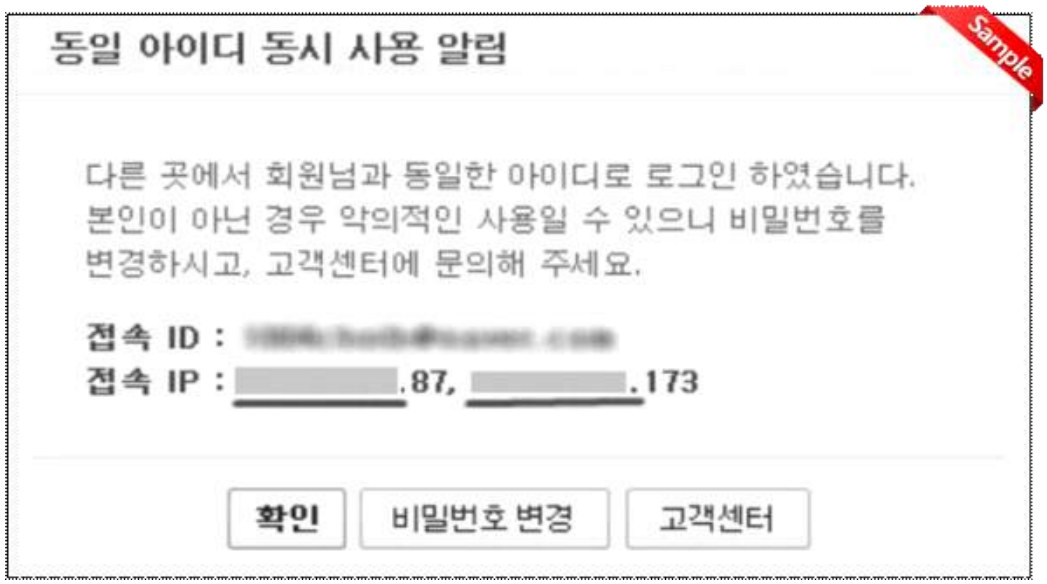
<서면 인사이동 및 퇴직 점검표>

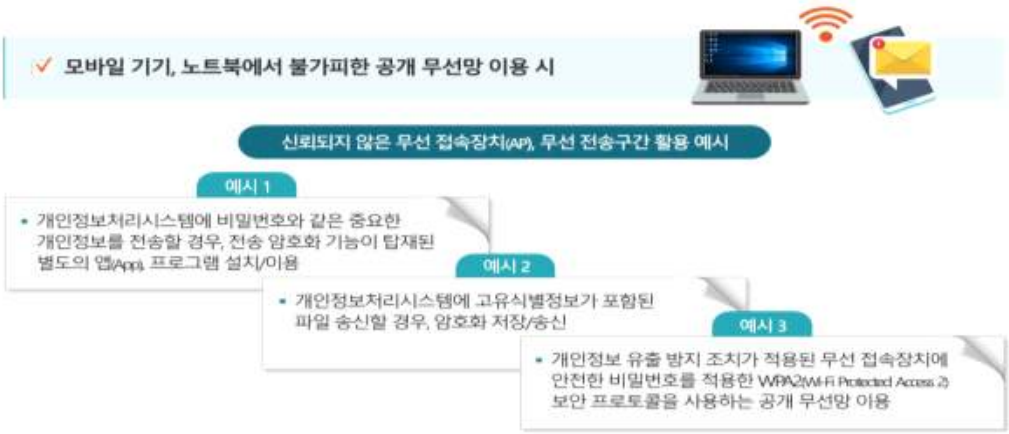
참고 자료

개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p263
개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p47
이미지 출처: 교육부, "교육정보시스템 권한부여 핸드북(나이스, K-에듀파인)", p6, p24

5	개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지 않는지 여부

③ 증빙자료 제출 항목(3/4)

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 개인정보 처리내역에 대한 책임 추적 성을 확보
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 시스템 상에서 제한하고 있는지 확인합니다.
점검 기준	◦ 미조치 : 사용자계정을 다른 개인정보취급자 등과 공유하는 경우 ◦ 해당없음 : 없음
증빙 자료	**1. 나이스 시스템, K-에듀파인 등 개인정보처리시스템 계정 동시사용 불가 화면 <필수>** 
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

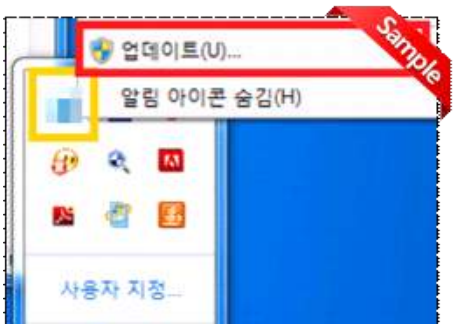
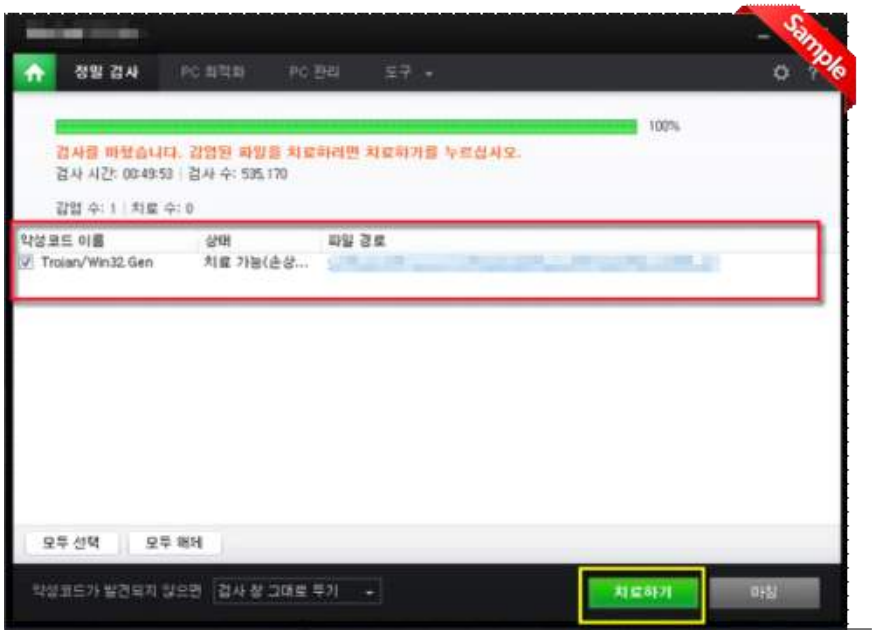
6	**개인정보가 인터넷 홈페이지, P2P, 공유설정 등으로 유·노출되지 않도록 개인정보처리시스템, 업무용컴퓨터 등에 접근통제 등에 관한 조치를 하고 있는지 여부**
관련 규정	**개인정보의 안전성 확보조치 기준 제6조(접근통제)** **→ 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치하는지 확인**
점검 방법	1. P2P, 웹하드, 공유설정 등 사용가능 확인 1) 원칙적으로 P2P 사용은 금지됩니다. 망분리를 하지 않은 경우 모든 P2P와 웹하드에 대해 통제하기 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

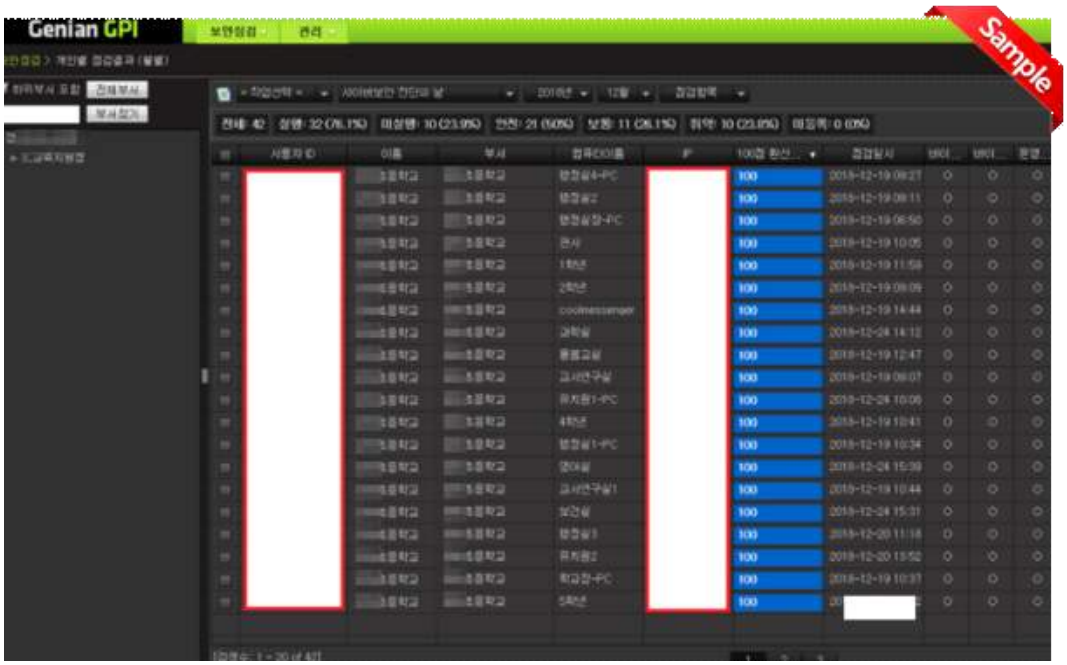
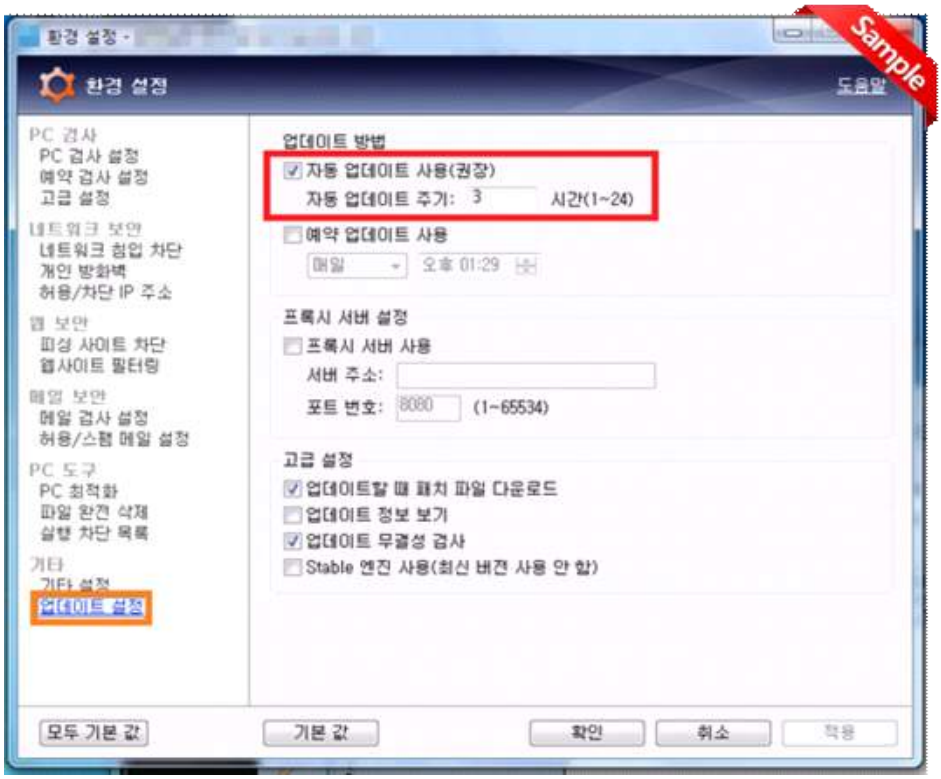
7	고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는지 여부
관련 규정	**개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)** **→ 고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우 안전한 알고리즘에 의한 암호화 조치하는지 여부**
점검 방법	1. 정보통신망을 통하여 송·수신하는 고유식별정보를 확인합니다. 1) SSL 적용 또는 안전한 암호화 알고리즘을 사용하여 송·수신하는 고유식별정보를 암호화하는지 확인합니다. 2) 시스템이 없는 경우에도 고유식별정보가 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)"

8	**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	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
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

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

④ 증빙자료 제출 항목(4/4)

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. 내PC지키미 관리자 프로그램 보안점검 결과 화면 <필수>**  **2. 내PC지키미를 사용하지 않는 경우, 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 이미지 출처: 울산광역시교육청, "내PC 지키미 관리자 매뉴얼(2019)" p11

10	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 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
참고 자료	개인정보보호위원회, "개인정보보호 법령 및 지침·고시 해설서(2020.12)", p269 개인정보보호위원회, 한국인터넷진흥원, "개인정보의 안전성 확보조치 기준 해설서(2020.12)", p79~80