고유식별정보 안전성 확보조치 관리실태 조사 매뉴얼

[민간기관용]

2018년 6월

행정안전부

KISA 한국인터넷진흥원

목 차

1. 참고 및 유의사항 ····· 3

2. 관리실태 조사 관련 FAQ ····· 4

3. 시스템 접속 ····· 6

4. 기관현황 등록 ····· 9

5. 자체점검 ····· 15

5.1. 용어의 정의 ····· 15

5.2. 세부항목별 점검방법 ····· 17

6. 기관현황 및 점검결과 수정 ····· 35

1. 참고 및 유의사항

1. **민간기관의 경우 본인인증 과정을 거쳐야 기관현황 등록 및 자체점검을 진행하실 수 있습니다. 기관현황 및 자체점검 결과의 수정 등 원활한 관리를 위해서는 1개 기관 당 여러 명의 담당자가 중복하여 등록하는 일이 발생하지 않도록 주의 부탁드리겠습니다.**

☞ 1개 기관 당 1명의 담당자가 1개의 결과를 제출

2. **자체점검 결과의 최종 제출일은 '18. 7. 31.(화)입니다.**

최종 제출일 전까지는 점검항목별 조치결과에 대한 수정이 가능하오니, 미 조치된 사항은 해당기한까지 조치를 완료하여 반영 부탁드립니다.

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

3. **자체점검의 점검항목은 「개인정보 보호법」 및 「개인정보의 안전성 확보조치 기준」에 따른 내용입니다.**

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」또는 「신용정보의 이용 및 보호에 관한 법률」의 적용을 받는 대상기관은, 「개인정보의 기술적·관리적 보호조치 기준」,「기술적·물리적·관리적 보안대책 마련 기준」등에서 규정하고 있는 사항을 준수하고 있을 경우 대부분의 점검항목 기준을 만족할 수 있습니다. 다만, 「개인정보의 기술적·관리적 보호조치 기준」,「기술적·물리적·관리적 보안대책 마련 기준」등에서 규정하고 있지 않은 사항에 대해서는 「개인정보의 안전성 확보조치 기준」규정을 준수하여야 합니다.

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

5. **자체점검 진행시 참고자료 목록**

(개인정보보호 종합포털 → 자료실 → 지침자료에서 다운로드 가능)

- **고유식별정보 안전조치 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

6. **관련문의 : 고유식별정보처리자 안전성 확보조치 관리실태 조사 사무국**

unique@kca21.com, 02-532-8841, 8847, 8851

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

2. 관리실태 조사 관련 FAQ

FAQ

▪ 처리하는 고유식별정보가 없음에도 관리실태 조사 대상인가요?

▪ 관리실태 조사는 임직원의 고유식별정보까지 포함하여, 민간의 경우 5만 명 이상 정보주체의 고유식별정보를 처리하여야만 조사 대상에 해당하나, 공공기관은 보유량에 따른 기준 없이 개인정보보호법에 따른 공공기관이면 모두 조사 대상에 해당합니다.

FAQ

▪ 관리실태 조사 대상기관에 해당합니다. 대상기관에 해당할 경우, 기관현황 및 자체점검 결과만 등록하면 되는 것인가요? 그 이후에 추가적으로 해야 하는 것은 없나요?

▪ 관리실태 조사 대상기관에 해당할 경우에는, 개인정보보호 종합포털(privacy.go.kr)에 접속한 후, 고유식별정보 보유현황 등 기관현황에 대한 정보를 등록하고, 안전성 확보조치 이행여부 확인을 위한 자체점검을 진행· 결과를 등록하면 됩니다. 대상기관이 기관현황 및 자체점검 결과를 '18.7.31. 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 7월 이후 개별안내)

FAQ

▪ 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.

FAQ ▪ 개인정보처리시스템에 있는 고유식별정보만 조사대상에 해당 하나요?

▪ 관리실태 조사는 개인정보처리시스템에 있는 고유식별정보 뿐만 아니라 종이문서, PC내 업무용 파일에 있는 고유식별정보까지 모두 포함됩니다. 임직원 정보가 있는 내부 개인정보처리시스템 또한 고유식별정보가 있다면 조사 대상에 해당합니다.

FAQ 현장점검을 받게 되는 기준은 무엇이며, 언제부터 진행 예정인가요?

▪ 현장점검은 관리실태 조사 대상기관 임에도 불구하고 '18.7.31.까지 기관현황 및 자체점검 결과를 등록하지 않은 기관, 대량 고유식별정보 처리기관, 증빙자료 검토결과 시정요구를 받은 기관, 기타 안전조치 미비기관 등 현장점검이 필요하다고 판단되는 기관 등을 대상으로 진행될 예정이며, 점검 일정은 9월부터 11월까지입니다. 다만, 상기 기준 및 일정은 상황에 따라 변동될 수 있습니다.

3. 시스템 접속

① 개인정보보호 종합포털(https://www.privacy.go.kr)에 접속합니다.

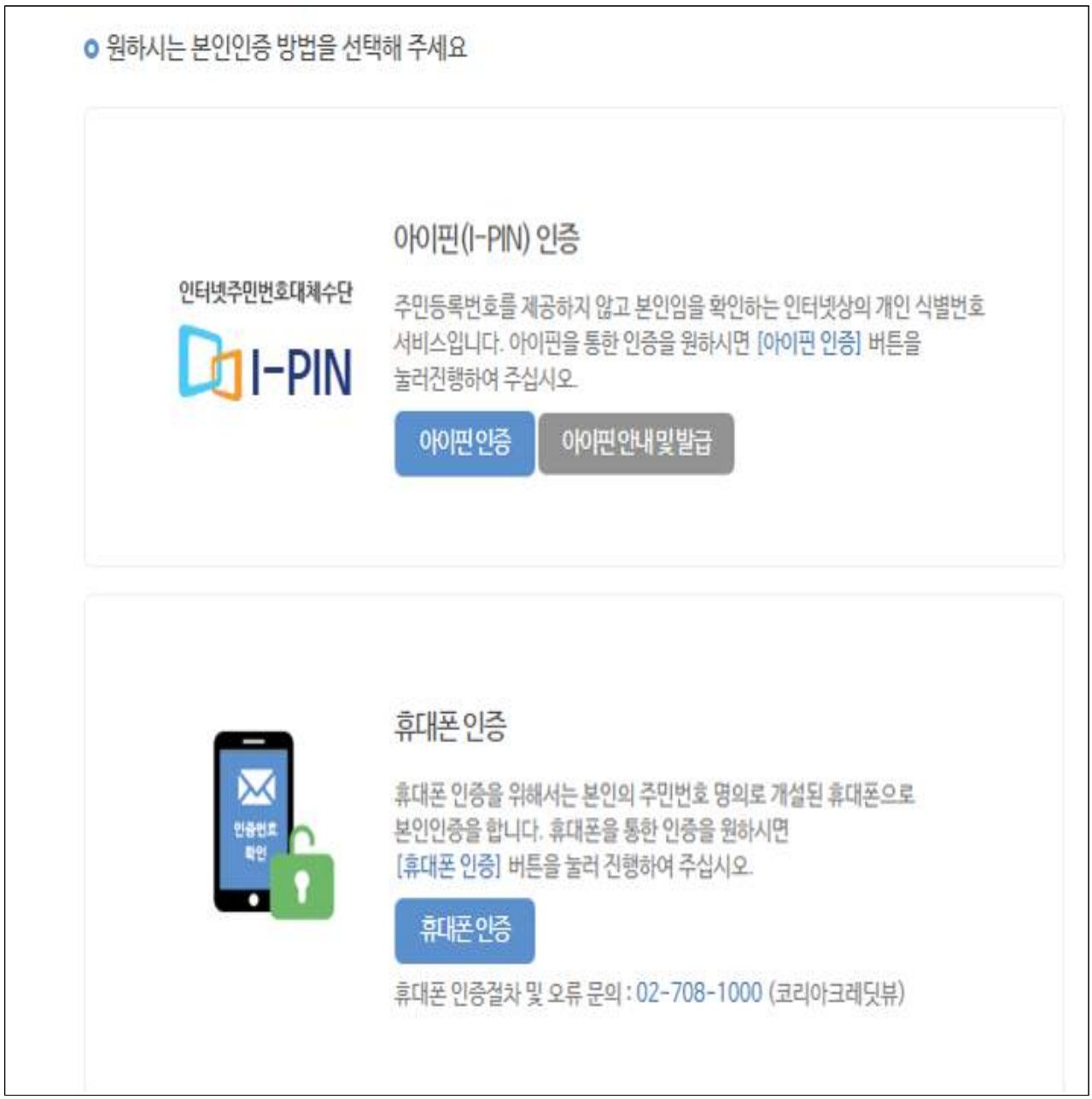
② 메인화면에서 자주 찾는 서비스 "고유식별정보 안전성 확보조치 실태조사" 아이콘 또는 팝업의 [바로가기 버튼]을 선택합니다.



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 대상기관 별 복수등록이 되지 않으므로, 최초 대상기관의 개인정보 보호 담당자 또는 실태조사 담당자가 본인인증절차 등 실태조사 관련 사항을 진행할 수 있도록 협조 부탁드립니다.

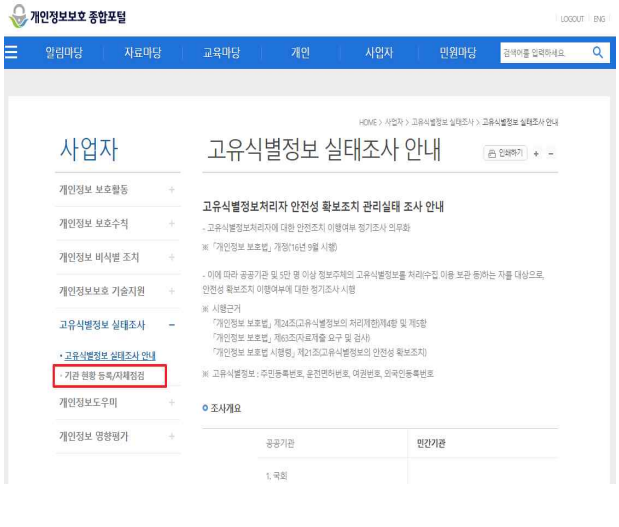
4. 기관현황 등록

(개인정보보호 종합포털 → 고유식별정보 실태조사(기관현황/자체점검) → 본인인증)

위의 과정에 따라 본인인증 절차가 완료되면, 기관현황 등록 페이지로 전환됩니다.



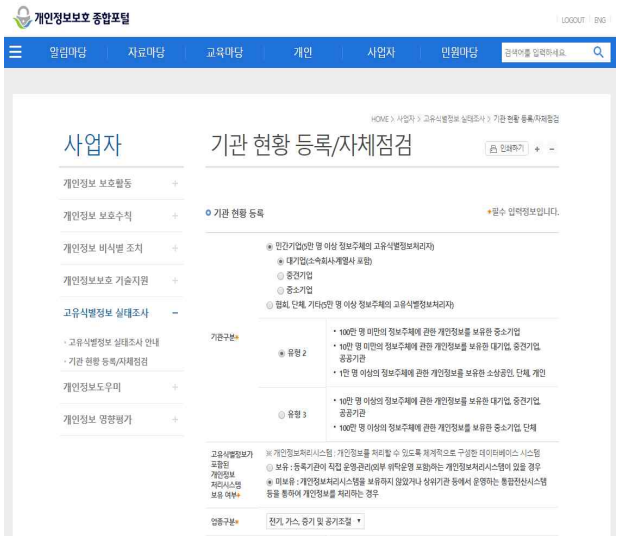
1. 개인정보보호 종합포털에서
고유식별정보 바로가기 클릭



2. 고유식별정보 안내페이지에서
기관현황등록/자체점검 클릭



3. 본인인증



4. 기관현황 및 자체점검 작성

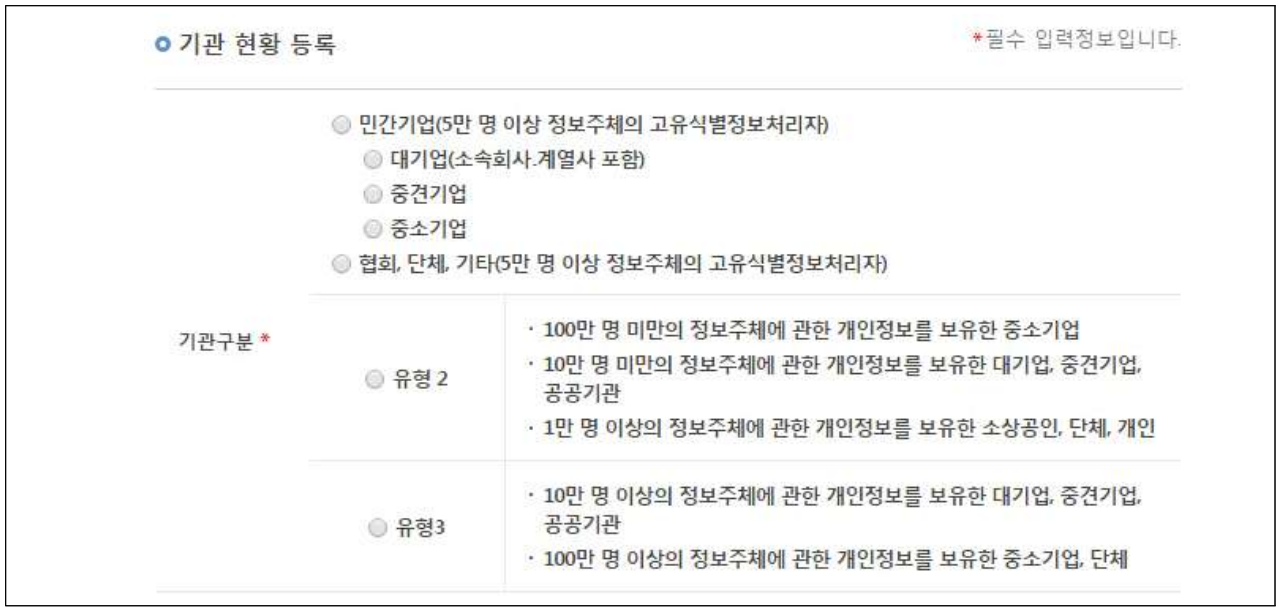
자체점검 페이지가 나타나면 기관 세부현황에 대하여 선택하고 관련정보를 입력합니다.



① 기관구분

: 민간 기업에 해당할 경우에는 대기업, 중견기업, 중소기업 중 선택하여 입력하고, 아닐 경우에는 협·단체·기타를 선택 합니다.

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



참고사항

■「개인정보 보호법」 제2조(정의) "공공기관"

6. "공공기관"이란 다음 각 목의 기관을 말한다.

가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체

나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관

■ 민간 기업의 구분('18년 4월 현재기준)

- (대기업, 중견기업, 중소기업) **개인정보의 안전성 확보조치 기준 해설서 21p~24p 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 보유건수가 아닌 개인정보를 보유하고 있는 정보주체의 수를 말함

※ 개인정보의 안전성 확보조치 기준

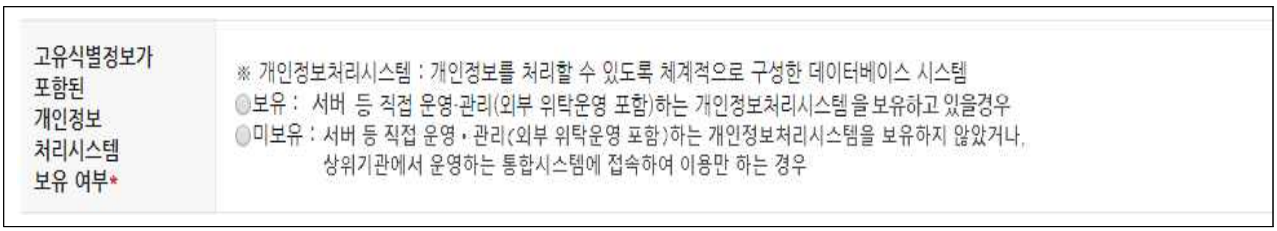
[별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준 참조

② 고유식별정보가 포함된 개인정보처리시스템 보유여부

: 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 보유여부를 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 응용프 로그램이 설치·운영되지 않는 PC, 노트북과 같은 업무용 컴퓨터는 개인정보처리시스템에서 제외)

③ 업종

: 대상기관이 해당하는 업종을 선택하여 입력합니다.

※ 통계청 : 한국표준산업분류의 대분류 참고

A. 농업, 임업 및 어업	B 광업
C 제조업	D 전기, 가스, 증기 및 공기조절 공급업
E 수도, 하수 및 폐기물 처리, 원료 재생업	F 건설업
G 도매 및 소매업	H 운수 및 창고업
I 숙박 및 음식점업	J 정보통신업
K 금융 및 보험업	K 금융 및 보험업
L 부동산업	M 전문, 과학 및 기술서비스업
N 사업시설 관리, 사업 지원 및 임대 서비스업	O 공공행정, 국방 및 사회보장 행정
P 교육서비스	Q 보건업 및 사회복지 서비스업
R 예술, 스포츠 및 여가관련 서비스업	S 협회 및 단체, 수리 및 기타 개인 서비스업
T 가구 내 고용활동, 자가소비 생산활동	U 국제 및 외국기관
v 기타	

④ 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.



⑤ 고유식별정보 보유현황

: 대상기관에서 현재 보유하고 있는 고유식별정보의 종류와 건수를 입력합니다.

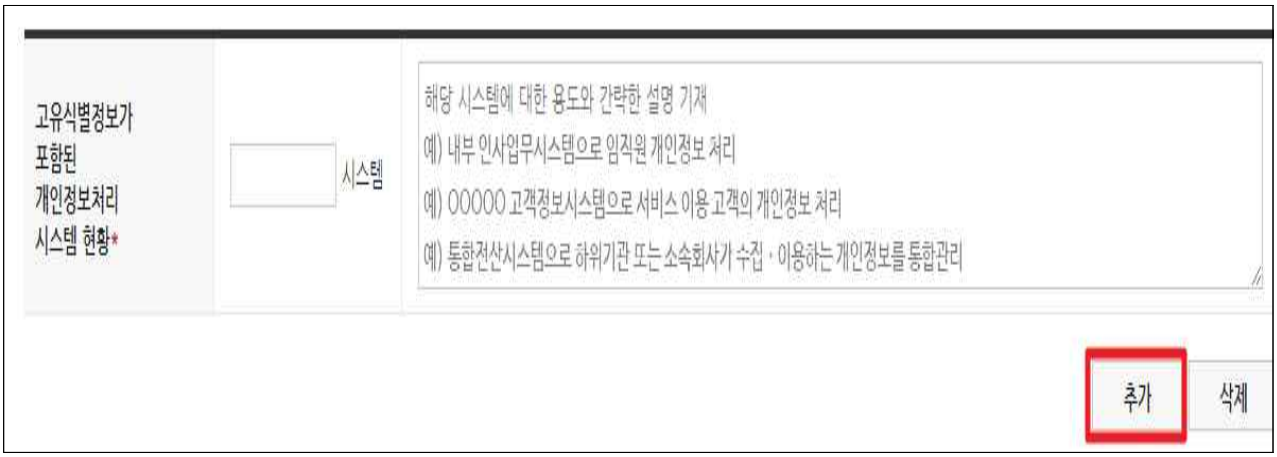
※ 고유식별정보 보유건수는 정보주체의 구분 없이 대상기관에서 보유하고 있는 고유식별정보에 대한 총 보유량을 기재합니다. (1종 이상 복수 선택가능)



⑥ 고유식별정보가 포함된 개인정보처리시스템 현황

: ②번 항목에서 개인정보처리시스템 미 보유 선택 시에는 비활성화 됩니다. 대상기관이 현재 보유하고 있는 개인정보처리시스템에 대한 명칭과 용도에 대하여 간략하게 기재합니다.
고유식별정보를 단 1건이라도 처리하는 시스템은 개인정보처리시스템으로 등록하며, 보유여부에 따라 [추가]버튼을 클릭하여 최대 50개까지 등록이 가능합니다.

[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, '자제점검' 화면으로 전환됩니다.)

※ 개인정보처리시스템 보유여부(보유·미보유)에 따라 자체점검 항목에 차이가 있으므로, 기관현황 등록이 완료되어야만 자체점검을 진행하실 수 있습니다. 해당 사항에 대하여 충분히 파악한 이후 현황등록을 진행하여 주시기 바라며, **기관현황은 등록이 완료된 이후에도 6월 말 자체점검 결과와 함께 수정이 가능합니다.**

5. 자체점검

※ 자체점검 결과등록은 대상기관 담당자 1명이 결과를 취합하여 등록

5-1. 용어의 정의

다음 용어에 대한 정의는 「개인정보 보호법」[법률 제14107호] 및「개인정보의 안전성 확보조치 기준」[행정안전부고시 제2016-35호]을 참조하였습니다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

2. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

4. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

6. “대기업”이란 「독점규제 및 공정거래에 관한 법률」제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.

7. “중견기업”이란「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」제2조에 해당하는 기업을 말한다.

8. “중소기업”이란 「중소기업기본법」제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.

9. “소상공인”이란 「소상공인 보호 및 지원에 관한 법률」제2조에 해당하는 자를 말한다.

10. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.

11. “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
12. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.

13. “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.

14. “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.

15. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

16. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

17. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.

18. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

19. “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.

20. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

21. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

22. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

※ 용어에 대한 세부 설명은 “개인정보의 안전성 확보조치 기준 해설서”(2017.1.) 14page ~ 25page 참조

5-2. 세부항목별 점검방법

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

1 주민등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거가 있는지 여부

[점검항목 설명]

고유식별정보 중 주민등록번호와 관련하여서는 2013. 8. 6. 개인정보 보호법 개정(2014. 8. 7. 시행)에 따라 원칙적으로 처리가 금지되고, 다음 사유에 해당하는 예외적인 경우에만 허용되고 있습니다.

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 안전행정부령으로 정하는 경우

따라서 위에서 정하는 예외사유에 해당되지 않는 한 주민등록번호를 수집하여 이용하거나, 제3자에게 제공하거나, 저장·보유하는 것이 모두 금지되고, 이는 정보주체로부터의 동의를 받는 경우에도 마찬가지입니다.(개정 이전에는 다른 고유식별정보와 같이 별도의 동의를 받으면 처리 가능하였으나, 현재는 불가능)
예외사유에 해당하는 한 정보주체로부터 별도의 동의를 받을 필요는 없습니다.

[점검방법]

현재 대상기관에서 보유하고 있는 주민등록번호에 대한 (법령상) 처리근거를 확인하여 점검결과에 반영합니다.

[관련규정]

■ 「개인정보 보호법」제24조의2(주민등록번호 처리의 제한)

2 여권번호, 운전면허번호, 외국인등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거 또는 정보주체의 동의가 있는지 여부

[점검항목 설명]

고유식별정보는 원칙적으로 처리할 수 없습니다. 다만, 별도로 정보주체의 동의를 받은 경우와 법령에서 고유식별정보의 처리를 요구하거나 허용하고 있는 경우에는 고유식별정보를 처리할 수 있습니다.
(다만, 고유식별정보 중 주민등록번호의 처리에 관하여서는 개인정보 보호법 제24조의2에서 별도 규정하고 있습니다)

정보주체에게 별도의 동의를 받는 경우에 개인정보처리자는 개인정보 보호법 제15조 제2항 각 호 또는 제17조 제2항 각 호의 사항을 정보주체에게 알리고 다른 개인정보의 처리에 대한 동의와 분리해서 고유식별정보 처리에 대한 동의를 받아야 합니다.
법령에서 구체적으로 처리를 요구하거나 허용하는 경우란, 원칙적으로 법령에서 구체적으로 고유식별정보의 종류를 열거하고 그 처리를 요구하거나 허용하고 있는 것을 말합니다. '법령'에 의한다고 규정하고 있으므로 법률 외에 시행령, 시행규칙이 포함되며 이에 첨부된 별지 서식이나 양식도 포함됩니다.

[점검방법]

현재 대상기관에서 보유하고 있는 주민등록번호를 제외한 고유식별정보가 법령의 근거에 의하여 처리하고 있는 것인지, 정보주체의 동의를 획득하여 처리하고 있는 것인지(동의를 획득하였다면 별도 동의절차를 준수하였는지) 등에 대하여 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제15조(개인정보의 수집.이용)
- 「개인정보 보호법」제24조(고유식별정보의 처리제한)
- 「개인정보 보호법 시행령」제19조(고유식별정보의 범위)

3 수집목적이 달성되었고, 보존기간이 경과한 고유식별정보를 파기하고 있는지 여부

[점검항목 설명]

개인정보처리자는 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기하여야 합니다.. "개인정보가 불필요하게 되었을 때"란 개인정보의 처리목적이 달성되었거나, 해당 서비스의 폐지, 사업이 종료된 경우 등이 포함됩니다. 따라서 개인정보처리자는 처리목적이 달성되거나, 해당 서비스 및 사업이 종료된 경우, 정당한 사유가 없는 한 5일 이내에 개인정보를 파기하여야 합니다.

다만 개인정보처리자는 '다른 법령에 따라 보존해야 하는 경우'에는 예외적으로 개인정보를 파기하지 않아도 됩니다. 개인정보처리자가 개인정보를 파기하지 않고 보존하려고 하는 경우에는 그 법적 근거를 명확히 해야 하며, 법령에 따라 개인정보를 파기하지 않고 보존하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 법령에서 보존하도록 한 목적 범위 내에서만 처리 가능하도록 관리하여야 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

[점검방법]

현재 대상기관에서 보유하고 있는 고유식별정보가 정보주체에게 동의 받은 보유기간을 경과하였거나 다른 법령에 따른 보존기간을 경과 하였음에도 불구하고 파기하지 않고 있는 것은 아닌지 확인하여, 점검 결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제21조(개인정보의 파기)
- 「개인정보 보호법 시행령」제16조(개인정보의 파기방법)
- 표준 개인정보보호지침 제10조(개인정보의 파기방법 및 절차
- 표준 개인정보보호지침 제11조(법령에 따른 개인정보의 보존)

4 개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행하고 있는지 여부

[점검항목 설명]

개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적.관리적 및 물리적 안전조치에 관한 내부 관리계획을 수립하고 시행하여야 합니다. 내부 관리계획에는 다음의 사항을 포함하여 수립합니다.

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. 접근 통제에 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

내부 관리계획은 전사적인 계획 내에서 개인정보가 관리될 수 있도록 최고경영층으로부터 내부결재 등의 승인을 받아 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 합니다.

[점검방법]

개인정보의 안전한 처리를 위한 내부 관리계획이 수립되어, 해당 계획에 따라 시행하고 있는지 확인하여 점검결과에 반영합니다.

※ 유형 2에 해당하는 대상기관은 위 12번~14번까지 항목은 내부 관리계획에 포함하지 않을 수 있습니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립.시행)

5 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는지 여부

[점검항목 설명]

개인정보처리자는 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 개인정보처리시스템에 대한 접근권한을 업무 수행 목적에 따라 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 접근통제를 위한 안전조치를 취해야 합니다.

특히, 개인정보처리시스템의 데이터베이스(DB)에 대한 직접적인 접근은 데이터베이스 운영·관리자에 한정하는 등의 안전조치를 적용할 필요성이 있습니다.

[점검방법]

개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 담당자에게 차등 부여하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

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

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

[점검항목 설명]

조직 내의 임직원 전보 또는 퇴직, 휴직 등 인사이동이 발생하여 사용자계정의 변경·말소 등이 필요한 경우에는 사용자계정 관리절차에 따라 통제하여 인가되지 않는 자의 접근을 차단하여야 합니다.

예를 들어, 직원의 퇴직 시 해당 직원의 계정을 지체 없이 변경·말소하는 조치 등을 내부관리계획 등에 반영하여 이행하도록 합니다. 또한, 직원의 퇴직 시 계정 말소를 효과적으로 이행하기 위해서는 퇴직 점검표에 사용자계정의 말소 항목을 반영하여, 계정 말소 여부에 대해 확인을 받을 수도 있습니다.

[점검방법]

개인정보취급자 변경 시, 개인정보처리시스템에 대한 접근권한을 지체 없이 변경 또는 말소하는 등의 조치를 취하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

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

7 개인정보처리시스템에 대한 개인정보취급자의 접근권한 부여·변경·말소 내역을 기록하고 3년간 보관하고 있는지 여부

[점검항목 설명]

개인정보처리자는 접근권한 부여·변경·말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 합니다.

예를 들어, 신청자 정보, 신청일시, 승인자 및 발급자 정보, 신청 및 발급 사유 등 접근권한의 발급 과정과 이력 등을 확인할 수 있도록 필요한 정보를 보관하여야 합니다.

[점검방법]

개인정보처리시스템에 대한 개인정보취급자의 접근권한 부여·변경· 말소 내역을 기록하고 3년간 보관하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

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

8 개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자와 공유하고 있지 않는지 여부

[점검항목 설명]

개인정보처리시스템에 접속할 수 있는 사용자계정은 개인정보취급자 별로 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 합니다.
다수의 개인정보취급자가 동일한 업무를 수행한다 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임 추적성(Accountability)을 확보하여야 합니다.

※ 책임 추적성이란 개인정보 취급에 따른 문제 발생 시 사 사용자계정을 기반으로 책임소재를 파악하는 것을 말함

[점검방법]

개인정보취급자별로 개인정보처리시스템에 대한 사용자계정을 발급하고, 해당 사용자계정을 공유하고 있지 않는지 확인하여 점검결과에 반영합니다.

[관련규정]

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

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

[점검항목 설명]

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

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

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

<비밀번호 작성규칙 예시>

· 비밀번호는 문자, 숫자의 조합.구성에 따라 최소 10자리 또는 8자리 이상의 길이로 설정
※ 기술 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있음
- 최소 10자리 이상: 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개), 특수문자(#, [, ", < 등, 32개) 중 2종류 이상으로 조합.구성한 경우
- 최소 8자리 이상: 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성한 경우

· 비밀번호는 추측하거나 유추하기 어렵도록 설정
- 일련번호(12345678 등), 전화번호, 잘 알려진 단어(love, happy 등), 키보드 상에서 나란히 있는 문자열(qwer 등) 등은 사용을 지양

· 비밀번호를 최소 6개월마다 변경하도록 변경기간을 적용하는 등 장기간 사용을 지양
- 변경 시 동일한(예시: Mrp15@*1aT와 Mrp15@*1at) 비밀번호를 교대로 사용하지 않도록 주의

[점검방법]

비밀번호 작성규칙을 수립하여 적용하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

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

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

[점검항목 설명]

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

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

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

[점검방법]

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

[관련규정]

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

11 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하고 있는지 여부

[점검항목 설명]

개인정보처리자는 개인정보처리시스템에서 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하기 위해 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소, 포트(Port), MAC(Media Access Control) 주소 등으로 제한하여 인가받지 않은 접근을 제한하도록 하여야 합니다.

[점검방법]

개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제6조(접근통제)

12 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 유출 시도를 탐지 및 대응하고 있는지 여부

[점검항목 설명]

개인정보처리자는 개인정보처리시스템에서 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하기 위해 개인정보처리시스템에 접속한 IP(Internet Protocol)주소, 포트(Port), MAC(Media Access Control) 주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지(침입탐지 기능)하고 접근 제한·차단 등 적절한 대응조치를 하여야 합니다.

<침입차단 및 침입탐지 기능을 갖춘 장비의 설치 방법 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 IP 주소 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

[점검방법]

개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 유출시도에 대하여 탐지 및 대응하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제6조(접근통제)

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

[점검항목 설명]

인터넷구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인정보처리자의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 합니다.

- 접속수단 예시: 가상사설망(VPN : Virtual Private Network) 또는 전용선 등

※ 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 지점간에 독점적으로 사용하는 회선으로 개인정보처리자와 개인정보취급자, 또는 본점과 지점간 직통으로 연결하는 회선 등을 의미

- 인증수단 예시: 인증서(PKI), 보안토큰, 일회용 비밀번호(OTP) 등

※ 인증서(PKI, Public Key Infrastructure) : 전자상거래 등에서 상대방과의 신원확인, 거래사실 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 한번만 사용가능하도록 하는 방식

[점검방법]

외부에서 개인정보처리시스템에 접속 시, 가상사설망, 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제6조(접근통제)

14 개인정보가 인터넷 홈페이지, P2P, 공유설정 등으로 유노출되지 않도록 개인정보처리시스템, 업무용컴퓨터 등에 접근통제 등에 관한 조치를 하고 있는지 여부

[점검항목 설명]

개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지 등을 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 합니다.

인터넷 홈페이지 중 서비스 제공에 사용되지 않거나 관리되지 않는 사이트 또는 URL(Uniform Resource Locator)에 대한 삭제 또는 차단 조치를 합니다.

인터넷 홈페이지의 설계·개발 오류 또는 개인정보취급자의 업무상 부주의 등으로 인터넷 서비스 검색엔진(구글링 등) 등을 통해 관리자 페이지와 취급중인 개인정보가 노출되지 않도록 필요한 조치를 합니다.

개인정보처리자는 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 P2P, 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 반드시 필요한 경우에는 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 합니다.

개인정보처리자는 공개된 무선망을 이용하여 개인정보를 처리하는 경우 취급중인 개인정보가 신뢰되지 않은 무선접속장치(AP), 무선 전송 구간 및 무선접속장치의 취약점 등에 의해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 하며, 다음과 같은 방식들을 활용 할 수 있습니다.

- 비밀번호 등 송신 시 SSL, VPN 등의 보안기술이 적용된 전용 프로그램을 사용하거나 암호화하여 송신
- 고유식별정보 등이 포함된 파일 송신 시 파일을 암호화하여 저장 후 송신
- 개인정보 유출 방지 조치가 적용된 공개된 무선망을 이용

[점검방법]

개인정보가 인터넷 홈페이지 등을 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 취하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제6조(접근통제)

15 인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우, 해당 홈페이지에 대해 연 1회 이상 취약점을 점검 및 그에 따른 개선조치를 하고 있는지 여부

[점검항목 설명]

인터넷 홈페이지를 통해(회원가입 등) 고유식별정보를 처리하는 개인정보처리자는 고유식별정보가 유출·변조·훼손되지 않도록 해당 인터넷 홈페이지에 대해 연 1회 이상 취약점을 점검하여야 하며, 그 결과에 따른 개선 조치를 하여야 합니다.

※ 웹 취약점 점검 항목 예시 : SQL_Injection 취약점, CrossSiteScript 취약점, File Upload 및 Download 취약점, ZeroBoard 취약점, Directory Listing 취약점, URL 및 Parameter 변조 등

인터넷 홈페이지의 취약점 점검은 개인정보처리자의 자체인력, 보안업체 등을 활용할 수 있으며, 취약점 점검은 상용 도구, 공개용 도구, 자체 제작 도구 등을 사용할 수 있습니다.

[점검방법]

고유식별정보를 처리하는 인터넷 홈페이지에 대하여 연 1회 이상 취약점 점검과 그에 따른 개선조치를 취하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제6조(접근통제)

16 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 개인정보처리시스템에 접속을 차단하고 있는지 여부

[점검항목 설명]

개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속의 차단을 의미하며, 업무용 컴퓨터의 화면보호기 등은 접속차단에 해당하지 않습니다.

개인정보취급자가 일정시간 이상 업무처리를 하지 않아 개인정보처리시스템에 접속이 차단된 이후, 다시 접속하고자 할 때에도 최초의 로그인과 동일한 방법으로 접속하여야 합니다.

[점검방법]

개인정보취급자가 일정시간 업무처리를 하지 않는 경우, 자동으로 개인정보처리시스템에 접속을 차단하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제6조(접근통제)

17 고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는지 여부

[점검항목 설명]

개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 합니다.

정보통신망을 통하여 고유식별번호를 송신하는 경우에는 SSL 등의 통신 암호 프로토콜이 탑재된 기술을 활용하거나, 암호화 응용프로그램을 활용하여 전송하는 정보를 암호화하여 송신하는 등의 방법을 사용할 수 있습니다.

※ SSL(Secure Sockets Layer)은 웹 브라우저와 웹 서버간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜



보조저장매체를 통해 고유식별정보를 전달하는 경우에도 암호화 하여야 하며, 이를 위해 다음과 같은 방법 등이 사용 될 수 있습니다.

- 암호화 기능을 제공하는 보안 USB 등의 보조저장매체에 저장하여 전달
- 해당 개인정보를 암호화 저장 한 후 보조저장매체에 저장하여 전달

※ 안전한 암호알고리즘, 암호화 방식 등은 "개인정보의 암호화 조치 안내서"를 참조하고, 해당 자료는 개인정보보호 종합포털(http://www.privacy.go.kr)에서 다운로드 가능

[점검방법]

고유식별정보를 송신 또는 보조저장매체를 통해 전달하는 경우, 안전한 알고리즘에 의한 암호화 조치를 취하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

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

[점검항목 설명]

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 결과에 관계없이 암호화 하여야 합니다. 이 경우에는 아래의 기간 이전까지 암호화 적용을 완료하여야 합니다.

※ 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일

※ 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

[점검방법]

내부망에 고유식별정보를 저장하는 경우 안전한 알고리즘을 통하여 암호화 조치를 취하고 있는지, 미 조치 중일경우에는, 영향평가나 위험도분석 결과를 따른 것인지 확인하여 점검결과에 반영합니다.

※ 영향평가 결과 또는 위험도분석 결과에 따른 암호화 미조치의 경우 자체점검 결과는 "조치"로 표시

※ 100만명 이상의 주민등록번호를 보관하는 개인정보처리자가 암호화 미조치 중일 경우, 영향평가 결과 또는 위험도분석 결과에 따른 것이면 "조치", 그렇지 않은 경우에는 "미조치"로 표시

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법」제24조의2(주민등록번호 처리의 제한)
- 「개인정보 보호법 시행령」제21조의2(주민등록번호 암호화 적용대상 등)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

19 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립 여부

[점검항목 설명]

암호 키는 암호화된 데이터를 복호화 할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 매우 중요하며, 라이프사이클 단계별 암호 키 관리 절차를 수립하여야 합니다.

※. 개인정보보호 종합포털(http://www.privacy.go.kr)에서 제공하는 "개인정보의 암호화 조치 안내서" 그리고 암호이용활성화(http://seed.kisa.or.kr)에서 제공하는 "암호 키 관리 안내서" 참고

[점검방법]

개인정보를 안전하게 보관하기 위한 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차가 수립되었는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

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

[점검항목 설명]

개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우에는, 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 이용하여 해당 파일을 암호화하여 불법적인 유·노출 및 접근 등으로부터 보호하여야 합니다.

<오피스에서 파일 암호화 설정방법>

· 한컴 오피스 : 파일 >> 다른이름으로 저장하기 >> 문서 암호 설정에서 암호 설정 가능 · MS 오피스 : 파일 >> 다른이름으로 저장하기 >> 도구 >> 일반옵션에서 암호 설정 가능

[점검방법]

업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우, 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화한 후 저장하는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

21 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하고 있는지 여부

[점검항목 설명]

개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속에 관한 이력정보를 최소 6개월 이상 보관·관리하여야 합니다.

[점검방법]

개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)

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

[점검항목 설명]

개인정보취급자가 개인정보처리시스템에 접속한 이력정보(접속기록)에는 아래의 사항이 포함되어야 합니다.

- 계정 : 개인정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID 등 계정 정보
- 접속일시 : 접속한 시간 또는 업무를 수행한 시간(년-월-일, 시:분:초)
- 접속자 정보 : 접속한 자의 PC, 모바일기기 등 단말기 정보 또는 서버의 IP주소 등
- 수행업무 : 개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용을 알 수 있는 정보

[점검방법]

개인정보취급자가 개인정보처리시스템에 접속한 이력정보(접속기록)에 사용자계정, 접속일시, 접속자정보, 수행한 업무내용 등이 포함되어 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)

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

[점검항목 설명]

개인정보처리자는 악성프로그램 등을 통해 개인정보가 위·변조, 유출되지 않도록 이를 방지하고 치료할 수 있는 백신 소프트웨어 등 보안 프로그램을 설치.운영하여야 하며,

백신 소프트웨어 등 보안 프로그램은 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지해야 합니다.

※ 실시간으로 키보드, 화면, 메모리해킹 등 신종 악성 프로그램이 유포됨에 따라 백신 상태를 항상 최신의 업데이트 상태로 적용하여 유지

[점검방법]

악성프로그램을 방지, 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치. 운영 및 최신의 상태로 유지하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제9조(악성프로그램 등 방지)

24 개인정보처리시스템에 직접 접속하는 관리용 단말기에 대해 비인가자가 임의로 조작하지 못하도록 조치하고 있는지 여부

[점검항목 설명]

개인정보처리자는 관리용 단말기에 대해 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 업무 처리를 하는 특정 직원 등에 한하여 접근을 허용하는 등 업무관련자 이외의 인가 받지 않는 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 접근통제 등의 안전조치를 하여야 합니다.

<관리용 단말기 안전조치 예시>

· 관리용 단말기 현황 관리(IP주소, 용도, 담당자, 설치 위치 등)
· 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 접근 통제
· 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지 등

[점검방법]

개인정보처리시스템에 직접 접속하는 관리용 단말기에 대해 비인가자가 임의로 조작하지 못하도록 조치를 취하고 있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제10조(관리용 단말기의 안전조치)

25 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있는지 여부

[점검항목 설명]

개인정보처리자는 개인정보가 포함된 서류, 보조저장매체(이동형 하드디스크, USB메모리, SSD 등) 등은 금고, 잠금장치가 있는 캐비넷 등 안전한 장소에 보관하여야 합니다.

[점검방법]

개인정보가 포함된 서류, 보조저장매체 등이 잠금장치가 있는 안전한 장소에 보관되어있는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제11조(물리적 안전조치)

26 재해·재난 발생 시, 개인정보의 손실·훼손 등을 방지하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 있는지 여부

[점검항목 설명]

개인정보처리자는 재해·재난 발생 시 개인정보의 손실 및 훼손 등을 방지하고 개인정보 유출사고 등을 예방하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 문서화하여 마련하여야 합니다.

※ 재난이란 국민의 생명.신체.재산과 국가에 피해를 주거나 줄 수 있는 것을 말하며, 재해란 재난으로 인하여 발생하는 피해를 말함

[점검방법]

개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하였는지 확인하여 점검결과에 반영합니다.

[관련규정]

- 「개인정보 보호법」제29조(안전조치의무)
- 「개인정보 보호법 시행령」제30조(개인정보의 안전성 확보조치)」
- [행안부 고시] 개인정보의 안전성 확보조치 기준 제12조(재해·재난 대비 안전조치)

6. 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 ~ 최종 제출일('18.7.31.)전 까지



기관 현황 등록 *필수 입력정보입니다.

기관구분*	민간기업> 대기업	
	유형2	
고유식별정보가 포함된 개인정보 처리시스템 보유 여부*	보유	
업종구분*	전기, 가스, 증기 및 공기조절 공급업	
기관정보*	기관명	(주)오더
	사업자등록번호	120-88-00767
	대표자명	이성수
	주소	서울시 서초구 방배로 111
담당자정보*	부서명	전략기획팀
	이름	홍길동
	회사 전화번호	02-1234-5678
	이메일	order@order.co.kr
고유식별정보 보유현황*	주민등록번호	23555 건
	여권번호	31662 건
	운전면허번호	123 건
	외국인등록번호	32 건
	합계	55372 건
고유식별정보가 포함된 개인정보처리 시스템현황*	홈페이지 회원관리 시스템	홈페이지 회원 관리를 위해 구축한 시스템
설문사항*	현장컨설팅 이용의향	있다

※ '고유식별정보 보유 현황'은 개인정보처리시스템 내 고유식별정보 건수, 업무파일, 종이문서 등 대상기관에서 보유하고 있는 모든 고유식별정보의 총 보유량을 정보주체 중복제거 없이 합산하여 총 건수를 입력
※ '고유식별정보가 포함된 개인정보처리시스템 현황'은 기관 담당자 1명이 취합하여 일괄등록
※ 고유식별정보를 단 1건이라도 보관하는 시스템은 개인정보처리시스템으로 등록
※ 지자체의 경우, 새올 등 공통시스템도 개인정보처리시스템 등록대상에 포함
※ 최대 50개 까지 등록가능

수정

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 유·노출되지 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, 접속자 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)

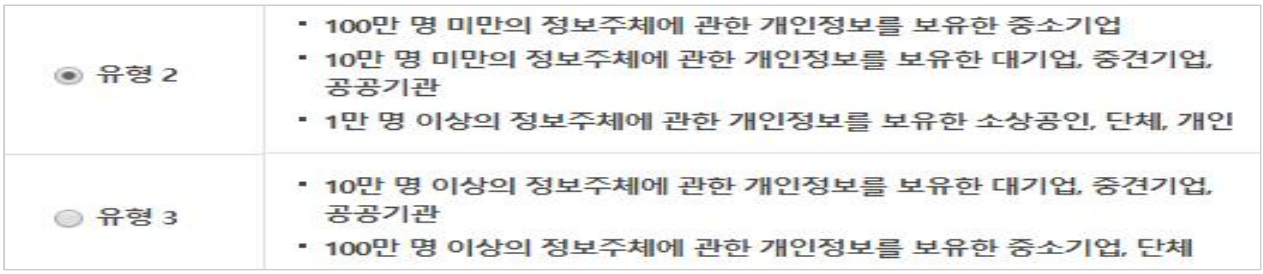
※ 상기 점검항목에서의 개인정보처리시스템은 고유식별정보가 포함된 개인정보처리시스템을 말함

※ 19,26번 항목은 유형3만 해당

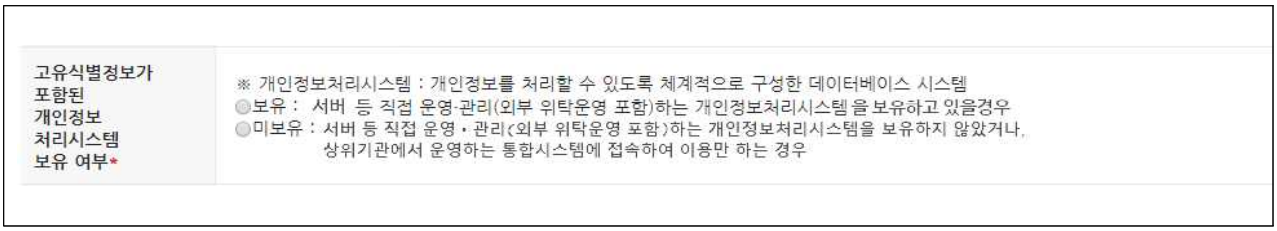
다운로드 인쇄 수정

※ 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 닫으신 경우에는 재접속 하신 후 자체점검 수정버튼을 눌러서 다시 작성해주세요