91812282 류재원

보호대책 요구사항

외부자보안

인증기준 & 인증목적

1. 업무의 일부(개인정보 취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터발생되는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.

2. 업무를 외부에 위탁하거나 외부의 시설 또는 서비스를 이용하는 현황을 식별함으로써 외부자로부터 발생할 수 있는 위험을 파악하고 적절한 보호 조치를 마련하기 위함이다.

※ 템플릿에 사용된 이미지는 홍보용입니다.

주요 확인사항

1. 관리체계 범위 내에서 발생하고 있는 업무 위탁 및 외부 시설·서비스의이용 현황을 식별하고 있는가?

2. 업무 위탁 및 외부 시설·서비스의이용에 따른 법적 요구사항과 위험을 파악하고 적절한 보호대책을 마련하고 있는가?

세부 설명

1. 관리체계 범위 내에서 발생하고 있는 업무 위탁 및 외부 시설·서비스의이용 현황을 명확히 식별하여야 한다.
 - 관리체계 범위 내 업무위탁 및 외부 시설·서비스 이용현황 파악
 - 업무위탁 및 외부 시설·서비스이용현황에 대한 목록 작성 및 지속적인 현행화 관리

2. 업무 위탁 및 외부 시설·서비스의이용에 따른 법적 요구사항과 위험을 파악하고 적절한 보호대책을 마련하여야 한다.
 - 개인정보 처리업무 위탁에 해당되는지 확인
 - 개인정보 등의 국외 이전에 해당되는지 확인
 - 개인정보 보호법, 정보통신망법 등 관련된 법적 요구사항 파악
 - 법적 요구사항을 포함하여 업무 위탁 및 외부 시설·서비스이용에 따른 위험평가 수행
 - 위험평가 결과를 반영하여 적절한 보호대책 마련 및 이행(예를 들어, 고위험의 수탁사에 대해서는 점검주기 및 점검항목을 달리하여 집중 현장점검 수행 등)

증거자료

1. 외부 위탁 및 외부 시설, 서비스 현황
2. 외부 위탁 계약서
3. 위험분석 보고서 및 보호대책
4. 위탁 보안관리 지침, 체크리스트 등

【붙임 1】

표준 개인정보처리위탁 계약서

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」 제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.

개인정보처리업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리위탁 계약서(안)

OOO(이하 "갑"이라 한다)과 △△△(이하 "을"이라 한다)는 "갑"의 개인정보 처리업무를 "을"에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 "갑"이 개인정보처리업무를 "을"에게 위탁하고, "을"은 승낙하여 "을"의 책임하에 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 개인정보보호법 시행령 및 시행규칙, 「표준 개인정보 보호지침」(행정안전부 예규 제25호)의 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "을"은 계약이 정하는 바에 따라 (_____)으로 다음과 같은 개인정보 처리 업무를 수행한다.1)

1.
2.

제4조 (재위탁 제한) ① "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 업무의 관리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.
② "을"이 재위탁받은 수탁회사를 선임한 경우 "을"은 당해 재위탁계약서와 함께 사실을 즉시 "갑"에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) "을"은 개인정보보호법 제29조, 동법 시행령 제 및 개인정보의 안전성 확보조치 기준 고시(행정안전부 고시 제2011-43호)에 따라 정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하는 안 된다.
② "을"은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리

개인정보관리 체크리스트

점 검			

■ 개인정보보호 정책 현황 [정책기반]

1. 개인정보보호 정책		예	아니오	해당없음
1 - 1	개인정보 보호를 위한 조직구성이 되어 있습니까?			
1 - 2	개인정보 보호책임자가 명확히 지정되어있습니까?			
1 - 3	개인정보 보호책임자가 역할 수행을 잘하고 있습니까?			
1 - 4	개인정보취급자가 관리적 지정되어 있습니까?			
1 - 5	개인정보 보호를 위한 심의위를 운영하고 있습니까?			
1 - 6	내부관리계획수립이 되어 있습니까?			
1 - 7	개인정보 보호조치 마련정신을 지속적으로 수행하고 있습니까?			

2. 개인정보보호 교육		예	아니오	해당없음
2 - 1	개인정보보호 교육계획 수립이 되어 있습니까?			
2 - 2	개인정보보호 책임자가 교육을 받고 있습니까?			
2 - 3	개인정보보호취급자(전직원, 계약직포함)에 대한 정기적인 교육을 수행하고 있습니까?			
2 - 4	수탁자에 대한 교육을 수행하고 있습니까?			

3. 개인정보보호 처리방침		예	아니오	해당없음
3 - 1	개인정보처리방침을 공개하고 있습니까?			
3 - 2	개인정보처리방침에 개인정보 관련 사항을 반영하고 있습니까?			
3 - 3	개인정보처리방침에 대한 지속점검 및 관리가 유지 되고 있습니까?			

4. 개인정보 영향평가		예	아니오	해당없음
4 - 1	개인정보영향평가 대상 시스템입니까?			
4 - 2	개인정보영향평가 수행계획수립이 되어 있습니까?			

■ 개인정보보호 정책현황 [기술기반]

5. 개인정보보호 시스템		예	아니오	해당없음
5 - 1	개인정보처리시스템 및 업무용컴퓨터에 백신 설치가 되어있습니까?			
5 - 2	백신소프트웨어에 대한 정기적인 업데이트를 수행하고 있습니까?			
5 - 3	침입차단시스템 또는 침입탐지시스템이 설치되어 운영되고 있습니까?			
5 - 4	웹 방화벽이 설치되어 운영 및 관리되고 있습니까?			
5 - 5	개인정보필터링이 설치되어 동작되고 있습니까?			

인증기준 & 인증목적

1. 외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.

2. 업무를 대행하는 외부자가 기업의 정보시스템, 네트워크, 인력 및 사무환경 등과 같은 정보자산에 접근할 때 관리, 통제의 보안 요구사항을 계약서나 특약에 명시해 정보보호에 관한 명확한 책임의 범위와 역할을 규정함으로써 문제 발생 시 명확한 처리가 가능하도록 하기 위함이다.

※ 템플릿에 사용된 이미지는 홍보용입니다.

주요 확인사항

1. 중요 정보 및 개인정보 처리와 관련된 외부 서비스 및 위탁 업체를 선정하는 경우 정보보호 및 개인정보 보호 역량을 고려하도록 절차를 마련하고 있는가?

2. 외부 서비스 이용 및 업무 위탁에 따른 정보보호 및 개인정보보호 요구사항을 식별하고 이를 계약서 또는 협정서에 명시하고 있는가?

3. 정보시스템 및 개인정보처리시스템 개발을 위탁하는 경우 개발 시 준수하여야 할 정보보호 및 개인정보보호 요구사항을 계약서에 명시하고 있는가?

세부 설명

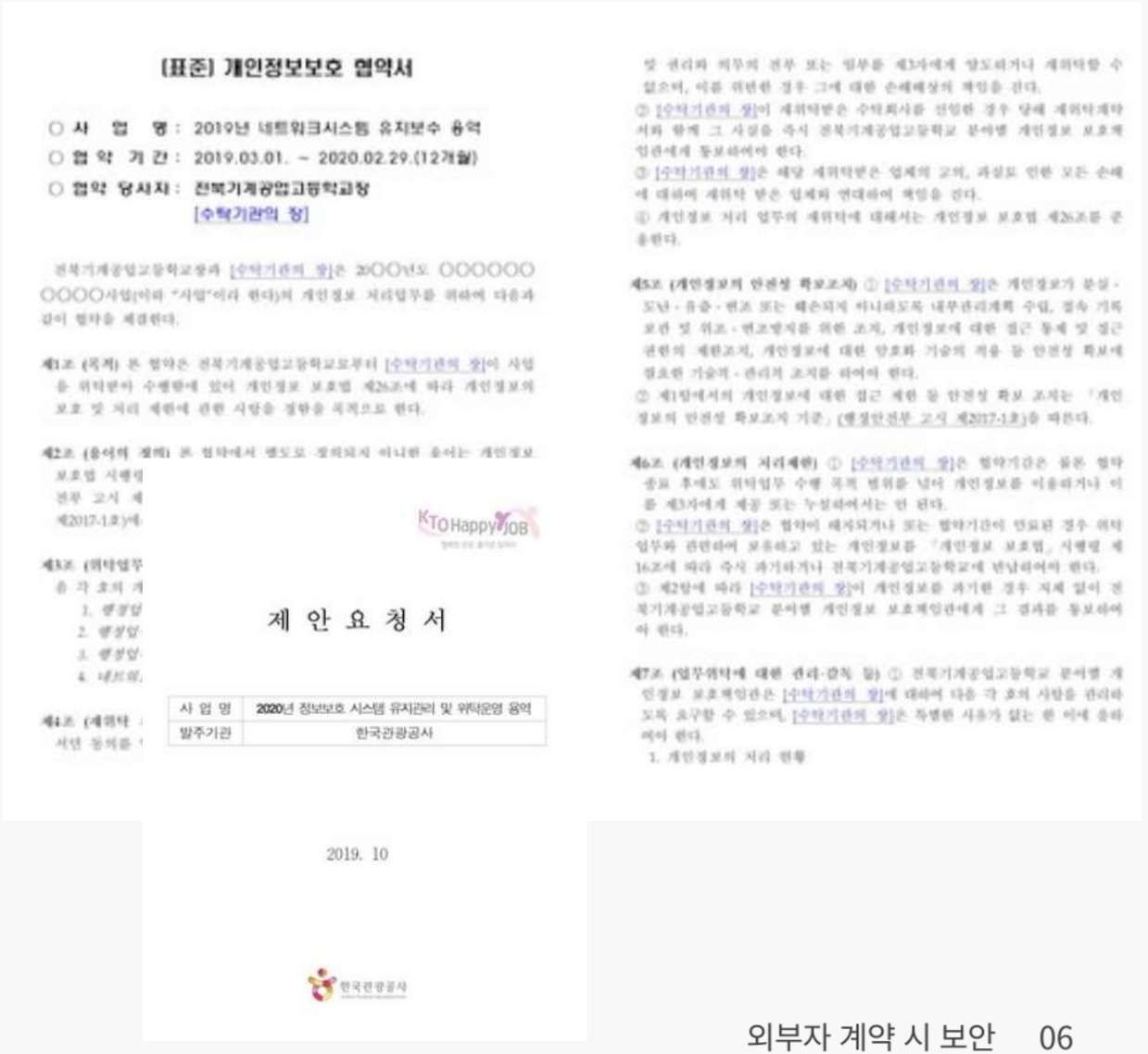
1. 주요정보 및 개인정보 처리와 관련된 외부 서비스 및 위탁 업체를 선정하는 경우 정보보호 및 개인정보 보호 역량을 고려하도록 절차를 마련하여야 한다.
 - 정보보호 및 개인정보보호 역량이 있는 업체가 선정될 수 있도록 관련 요건을 제안요청서(RFP) 및 제안 평가항목에 반영하여 업체 선정 시 적용

2. 조직의 정보처리 업무를 외부자에게 위탁하거나 외부 서비스를 이용하는 경우 다음과 같은 보안 요구사항을 정의하여 계약 시 반영하여야 한다(개인정보보호법 제26조 및 동법 시행령 제28조 참고).
 - 정보보호 및 개인정보보호 관련 법률 준수, 정보보호 및 개인정보보호 서약서 제출

3. 정보시스템 및 개인정보처리시스템 개발을 위탁하는 경우 개발 시 준수하여야 할 정보보호 및 개인정보 보호 요구사항을 계약서에 명시하여야 한다.
 - 정보보호 및 개인정보보호 관련 법적 요구사항 준수

증거자료

1. 위탁 계약서
2. 정보보호 및 개인정보보호 협약서(약정서, 부속합의서)
3. 위탁 관련 내부 지침
4. 위탁업체 선정 관련 RFP(제안요청서), 평가표



(표준) 개인정보보호 협약서

○ 사 업 명 : 2019년 네트워크시스템 유지보수 용역
○ 협 약 기 간 : 2019.03.01. ~ 2020.02.29.(12개월)
○ 협 약 당 사 자 : 전북기계공업고등학교장
[수탁기관의 장]

제 안 요 청 서

사 업 명	2020년 정보보호 시스템 유지관리 및 위탁운영 용역
발주기관	한국관광공사

2019. 10

한국관광공사

인증기준 & 인증목적

1. 계약서, 협정서, 내부 정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야한다.

2. 외부 인력을 통한 정보시스템의 개발, 운용, 정비 등의 업무 수행 시 고의나 실수로 인한 정보 유출, 훼손 등을 방지하고, 보안 요구사항에 대한 점검기준을 마련하기 위함이다.

※템플릿에 사용된 이미지는 홍보용입니다.

주요 확인사항

1. 외부자가 계약서, 협정서, 내부 정책에 명시된 정보보호 및 개인정보보호 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하고 있는가?

2. 외부자에 대한 점검 또는 감사 시 발견된 문제점에 대하여 개선 계획을 수립·이행하고 있는가?

3. 개인정보 처리 업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재위탁하는 경우 위탁자의 승인을 받도록 하고 있는가?

세부 설명

1. 외부자가 계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하여야 한다.
 - 외부자와 계약 시 정의한 보안 요구사항을 준수하고 있는지 주기적으로 점검, 감사 수행

2. 외부자에 대한 점검 또는 감사 시 발견된 문제점에 대하여 개선계획을 수립·이행하여야 한다.
 - 점검 및 감사 결과에 대하여 공유하고 발견된 문제점에 대한 개선방법 및 재발 방지대책을 수립하여 이행
 - 개선 조치 완료 여부에 대한 이행점검 수행

3. 개인정보 처리업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재위탁하는 경우 위탁자의 승인을 받도록 하여야 한다.
 - 개인정보 처리 수탁자는 위탁자의 동의를 받은 경우에 한하여 재위탁하고, 위탁자가 수탁자에게
요구하는 동일한 수준의 기술적·관리적보호조치를 재위탁자가 이행하도록 관리·감독

증거자료

1. 외부자 및 수탁자 보안점검 결과
2. 외부자 및 수탁자 교육 내역(교육 결과, 참석자 명단, 교육교재 등)
3. 개인정보 위탁 계약서

[붙임1 서식]

수탁업체 개인정보보호 교육 서명록(예시)

○ 교육일자 : 년 월 일
○ 교육장소 :
○ 교육내용 : 수탁업체 개인정보보호 준수사항

구분	업체명	직급	성명	서명
1	최고 보안업체	주임	홍 길 동	

해당 수탁업체 직원이 개인정보 교육을 받아 '교육확인서'를 제출 하였으면 '교육 서명록'은 안 받아도 됩니다.

[붙임2 서식]

수탁업체 개인정보보호 실태 점검표(예시)

유관에 대한 실태 점검표는 모두 '예'로 선택해주세요.

○ 업체명 : 최고 보안업체
○ 점검일자 : 년 월 일

순번	점검항목	점검결과		해당 없음	비고
		예	아니오		
1	내부관리계획의 수립 · 시행	V			
2	접근권한의 관리여부	V			
3	개인정보처리시스템의 접근관리 여부	V			
4	개인정보의 암호화(고유식별정보) 여부	V			
5	개인정보처리시스템의 접속기록 보관 및 점검 여부	V			
6	악성프로그램 등 방지 여부(백신 프로그램 설치 등)	V			
7	물리적 접근 방지 여부(통제절차, 잠금장치 등)	V			
8	개인정보의 파기	V			
9	재 위탁 여부	V			

※ 「개인정보의 안전성 확보조치 기준(행정자치부고시 제2014-7호)」 참조
※ 요양기관의 규모에 따라 점검항목의 조정 가능 함

인증기준 & 인증목적

1. 외부자 계약만료, 업무 종료, 담당자 변경 시에는 제공한 정보자산 반납, 정보시스템 접근계정 삭제, 중요 정보 파기, 업무 수행 중 취득 정보의 비밀유지 확약서 징구 등의 보호 대책을 이행하여야 한다.

2. 외부자와의 계약이 변경, 만료되거나 담당자가 변경되는 등의 변경사항이 발생하는 경우 계정 반납과 삭제, 비밀유지 확약서 등 필요한 보안 조치를 체계적으로 적응하도록 하기 위함이다.

※ 템플릿에 사용된 이미지는 홍보용입니다.

주요 확인사항

1. 외부자 계약만료, 업무 종료, 담당자 변경 시 공식적인 절차에 따른 정보자산 반납, 정보시스템 접근 계정 삭제, 비밀유지 확약서 징구 등이 이루어질 수 있도록 보안대책을 수립·이행하고 있는가?

2. 외부자 계약 만료 시 위탁 업무와 관련하여 외부자가 중요 정보 및 개인정보를 보유하고 있는지 확인하고 이를 회수·파기할수 있도록 절차를 수립·이행하고있는가?

세부 설명

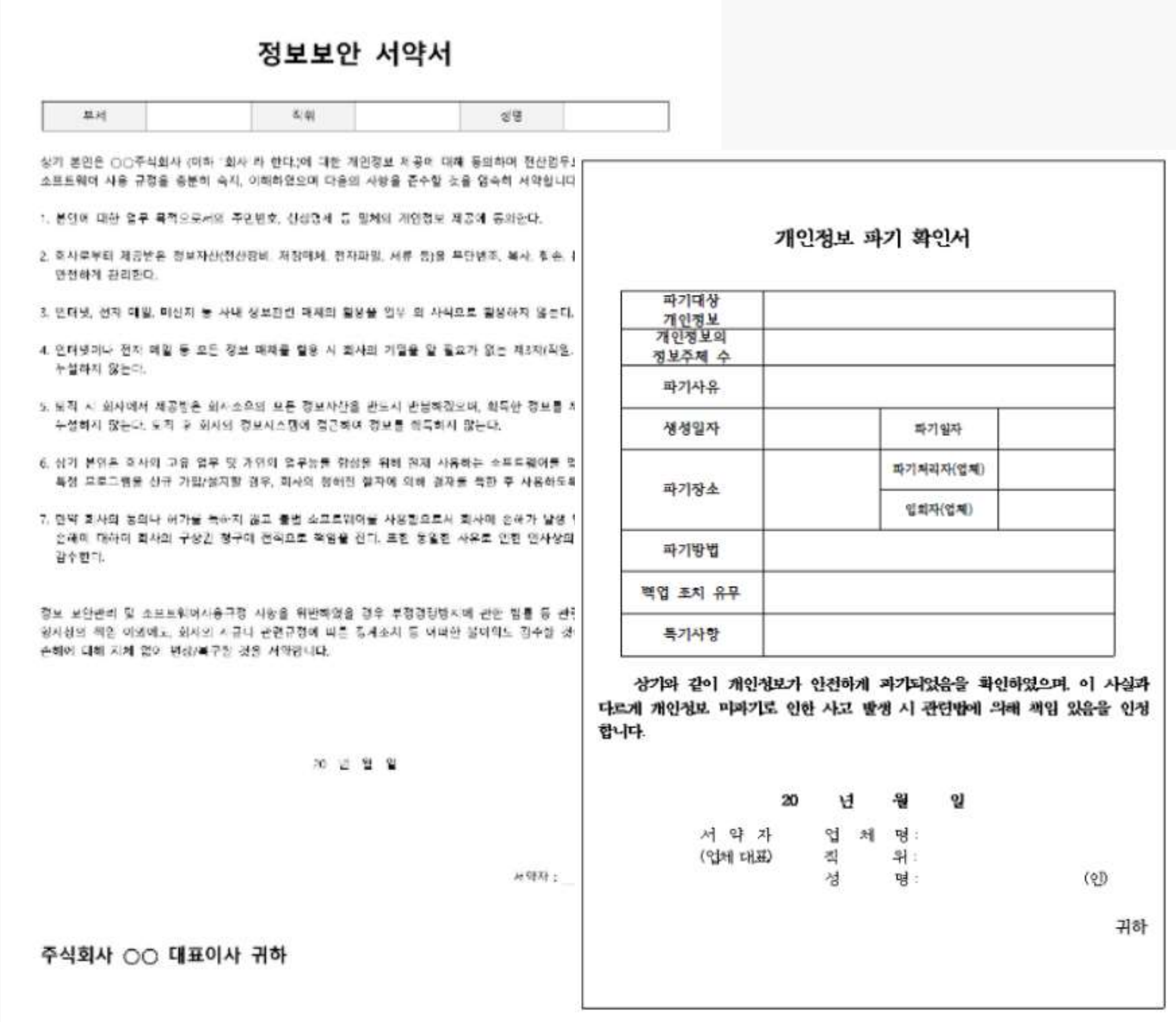
1. 외부자 계약만료, 업무 종료, 담당자 변경 시 공식적인 절차에 따른 정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 비밀유지 확약서 징구 등이 이루어질 수 있도록 보안대책을 수립·이행하여야한다.
 - 담당조직이 외부자 계약만료, 업무 종료, 담당자 변경이 발생하였음을 신속하게 인지할 수 있도록 정보공유 방안 마련
 - 외부자 계약만료, 업무 종료, 담당자 변경에 따른 보안대책 수립 및 이행

2. 외부자 계약 만료 시 위탁 업무와 관련하여 외부자가 중요정보 및 개인정보를 보유하고 있는지 확인하고 이를 회수·파기할수 있도록 절차를 수립·이행하여야한다.
 - 개인정보 등 중요정보를 회수·파기하기위하여 수탁사 직접 방문 또는 원격으로 개인정보를 파기한 후 파기 확약서 작성
 - 정보시스템과 담당자 PC뿐 아니라, 메일 송수신함 등 해당 정보가 저장되어 있는 모든 장치 및 매체에 대한 삭제 조치 필요
 - 해당 정보가 복구·재생되지않도록 안전한 방법으로 파기

04 외부자 계약 변경 및 만료 시 보안

증거자료

1. 정보보호 및 개인정보 서약서
2. 비밀유지 확약서
3. 정보 및 개인정보 파기 확약서
4. 외부자 계약 종료와 관련된 내부 정책, 지침



정보보안 서약서

부서		직위		성명	

상기 본인은 ○○주식회사 (이하 '회사'라 한다.)에 대한 개인정보 제공에 대해 동의하며 전산업무[illegible]
소프트웨어 사용 규정을 충분히 숙지, 이해하였으며 다음의 사항을 준수할 것을 엄숙히 서약합니다

1. 본인에 대한 업무 목적으로서의 주민번호, 신상명세 등 일체의 개인정보 제공에 동의한다.
2. 회사로부터 제공받은 정보자산(전산장비, 저장매체, 전자파일, 서류 등)을 무단변조, 복사, 훼손, [illegible] 안전하게 관리한다.
3. 인터넷, 전자 메일, 메신저 등 사내 정보전산 매체의 활용을 업무 외 사적으로 활용하지 않는다.
4. 인터넷이나 전자 메일 등 모든 정보 매체를 활용 시 회사의 기밀을 알 필요가 없는 제3자(직원, [illegible] 누설하지 않는다.
5. 퇴직 시 회사에서 제공받은 회사 소유의 모든 정보자산을 반드시 반납해야 하며, 획득한 정보를 [illegible] 누설하지 않는다. 퇴직 후 회사의 정보시스템에 접근하여 정보를 취득하지 않는다.
6. 상기 본인은 회사의 고유 업무 및 개인의 업무능률 향상을 위해 현재 사용하는 소프트웨어를 [illegible] 특정 프로그램을 신규 가입/설치할 경우, 회사의 정해진 절차에 의해 결재를 득한 후 사용하도록[illegible]
7. 만약 회사의 동의나 허가를 득하지 않고 불법 소프트웨어를 사용함으로서 회사에 손해가 발생 [illegible] 손해에 대하여 회사의 구상권 청구에 전적으로 책임을 진다. 또한 동일한 사유로 인한 인사상의 [illegible] 감수한다.

정보 보안관리 및 소프트웨어사용규정 사항을 위반하였을 경우 부정경쟁방지에 관한 법률 등 관련[illegible] 위 사항의 책임 이외에도, 회사의 사규나 관련규정에 따른 징계조치 등 어떠한 불이익도 감수할 것[illegible] 손해에 대해 지체 없이 변상/복구할 것을 서약합니다.

20 년 월 일

서약자 :

주식회사 ○○ 대표이사 귀하

개인정보 파기 확인서

파기대상 개인정보			
개인정보의 정보주체 수			
파기사유			
생성일자		파기일자	
파기장소		파기처리자(업체)	
		입회자(업체)	
파기방법			
백업 조치 유무			
특기사항			

상기와 같이 개인정보가 안전하게 파기되었음을 확인하였으며, 이 사실과 다르게 개인정보 미파기로 인한 사고 발생 시 관련법에 의해 책임 있음을 인정합니다.

20 년 월 일

서 약 자 (업체 대표) 업 체 명 :
직 위 :
성 명 : (인)

귀하

Thank You