

2026년 영양플러스사업 보충식품 공급

수탁업체 개인정보 관리 실태 점검표

부서명	건강증진과	점검기간	2026년 상반기
사업명	영양플러스사업	점검일	2026. 8. 4.
개인정보 보호책임자 (수탁자)	김 강 하 	점검자	신수연 (서명) 

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	여	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	여	
3	제 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	여	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	여	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	여	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	여	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	여	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	여	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	여	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	여	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	여	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	여	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	여	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설점 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	여	

15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	여	
16	악성프로그램 경보가 발령되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	여	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	여	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	여	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단·탐지 등 안전조치를 하고 있는가?	여	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	부	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	여	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	여	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	부	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	부	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 알고리즘으로 암호화하여 저장하고 있는가?	부	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	부	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	부	

2026년 모바일 워크온 걷기운동사업 운영

수탁업체 개인정보 관리 실태 점검표

부서명	스왈라비(주) 운영팀	점검기간	2026.01.01.~2026.12.31
사업명	2026 모바일 워크온 걷기 운동 사업 운영 관련 용역사업	점검일	2026.01.02
용역책임자(사업자)	정해권 (서명)	점검자	이호재 (서명)

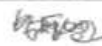
연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 사등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민간정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	○	

15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	○	
16	악성프로그램 경보가 발령되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	○	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	○	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	○	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단·탐지 등 안전조치를 하고 있는가?	○	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	○	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	○	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	○	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 알고리즘으로 암호화하여 저장하고 있는가?	○	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	○	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	○	

2026년 교하도서관 CCTV 유지보수

[붙임]

수탁업체 개인정보 관리 실태 점검표

부서명	교하도서관	점검기간	2026년
사업명	CCTV 유지보수	점검일	2026. 8. 26.
용역책임자(사업자)	(주)티원정보 	점검자	박명선 

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 임무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 금융정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	○	

15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	☐	
16	악성프로그램 경보가 발생되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	☐	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	☐	
18	개인정보취급자 또는 정보주체의 비밀번호, 등 인증수단을 안전하게 적용하고 관리하고 있는가?	☐	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단장치 등 안전조치를 하고 있는가?	☐	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	☐	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	☐	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	☐	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	☐	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	☐	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 알고리즘으로 암호화하여 저장하고 있는가?	☐	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	☐	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조제장 매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	☐	

2026년 교하도서관 RFID 유지보수

[붙임7]

수탁업체 개인정보 관리 실태 점검표

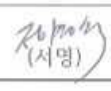
부서명	교하도서관	점검기간	2026년
사업명	RFID 유지보수	점검일	2026. 8. 26.
용역책임자(사업자)	(주)제이엔에스 	점검자	박명선 

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	새 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일 등 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 철회하고 있는가?	○	
8	개인정보처리시스템 접근 권한에 부여된 정보 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일자, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 일1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 때에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	
14	처리하는 개인정보가 인터넷 홈페이지, P2P 공유실행 등을 통하여 권한이 없는 사에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기의 조치를 하고 있는가?	○	

15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(악성 소프트웨어 등을 실차·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나)을 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	○	
16	악성프로그램 경보가 발생되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	○	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	○	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	○	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단·탐지 등 안전조치를 하고 있는가?	○	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안도른, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	○	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	○	
22	개인정보취급자가 일정시간 이상 업무사태를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	○	
23	비밀번호, 생체인식정보, 전자서명값, 인증도른 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(MZ), 내부망에 저장하는 경우, 안전한 알고리즘으로 암호화하여 저장하고 있는가?	○	
26	비밀번호, 생체인식정보, 전자서명값, 인증도른 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	○	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장 장치 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	해당없음	

2026 이동노동자 센터 운영 및 유지관리

수탁업체 개인정보 관리 실태 점검표

부서명	기업지원과	점검기간	2026. 1. 1. ~ 7. 31.
사업명	이동노동자센터 운영	점검일	2026. 8. 3.
용역책임자(사업자)	이사 정명석 (주식회사 오딘로보틱스) 	점검자	주무관 박은지 

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	X	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	해당없음	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	

14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	○	
15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	○	개인정보취급자 개인정보취급자
16	악성프로그램 정보가 발령되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	○	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	○	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	○	개인정보취급자 개인정보취급자
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단·탐지 등 안전조치를 하고 있는가?	○	개인정보취급자 개인정보취급자
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	○	개인정보취급자 개인정보취급자
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	X	개인정보취급자
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	○	개인정보취급자 개인정보취급자
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	개인정보취급자 개인정보취급자
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	개인정보취급자 개인정보취급자
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	해당없음	개인정보취급자 개인정보취급자
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	X	개인정보취급자 개인정보취급자
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	해당없음	개인정보취급자 개인정보취급자

문산 도서관 CCTV 유지보수

수탁업체 영상정보처리기기 관리실태 점검표

부서명	문산도서관	점검일	2026. 7. 21.
사업명	2026년 문산도서관 CCTV 유지보수 용역	점검자	김성진 김성진
용역책임자(사업자)	(주)티원정보 차장 은지우 (주)티원정보 대리 이관우		

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	X	
4	(위탁사 협의 시) 재 위탁하는 경우 수탁사가 관리·감독을 수행하는가?	○	
5	영상정보가 관리되는 PC, 시스템에 비인가 프로그램(P2P, 웹하드 등의) 접속을 차단하는가?	○	
6	영상정보에 접근할 수 있는 접근 권한의 제한 조치를 수행하고 있는가?	○	
7	개인영상정보를 안전하게 저장·전송할 수 있는 기술(암호화, 비밀번호 설정 등) 적용하고 있는가?	○	
8	영상정보파일 접근하는 PC 및 시스템에 비밀번호를 설정하여 관리하는가?	○	
9	개인영상정보 관리대장을 작성하고 있는가? · 영상정보 미저장 시 파일 대장 비치 여부	○	
10	영상정보의 보관 및 위조·변조에 대한 조치를 수행하고 있는가? (개인영상정보의 생성 일시 및 열람할 경우 목적·열람자·열람일시 등)	○	
11	계약종료에 따른 수탁사 계정 권한 말소 등 접근 권한 관리를 적절하게 관리하는가?	○	
12	수탁자가 처리한 영상정보를 반환·파기 등 사후 조치가 관리되고 있는가?	○	

2026년 부동산종합공부시스템 소프트웨어 유지보수

[붙임7]

수탁업체 개인정보 관리 실태 점검표

부서명	부동산과	점검기간	2026.01.01. ~2026.12.31.
사업명	부동산종합공부시스템유지보수	점검일	2026.8.28.
용역책임자(사업자)	(주)정도유아이티 	점검자	방해옥 

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	☐	62
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	☐	
3	새 입찰을 하거나 입찰 목적 외로 개인정보를 활용하지는 않는가?	☐	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	☐	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	☐	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에개인 업무 수행에 필요한 최소한의 범위로 자동 부여하고 있는가?	☐	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	☐	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	☐	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	☐	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 작성자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	☐	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	☐	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다용도도가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	☐	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	☐	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유실장 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	☐	

15	업무를 컴퓨터에 작성프로그램 등을 발차·처리할 수 있는 보안 프로그램(백신 소프트웨어 등을) 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	☐	
16	작성프로그램, 정보기 발령되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	☐	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정통 발급하고 있는가?	☐	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	☐	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단장치 등 안전조치를 하고 있는가?	☐	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	☐	42
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일상 필수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	☐	
22	개인정보취급자가 일정한시간 이상 업무차료를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	☐	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	☐	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	☐	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(CMZ, 내부망에 저장하는 경우, 안전한 알고리즘으로 암호화하여 저장하고 있는가?	☐	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	☐	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	☐	

2026년 파주시 공식 SNS 운영 용역

수탁업체 개인정보 관리 실태 점검표

부서명	소통홍보관	점검기간	2026. 1. 1. ~ 8. 31.
사업명	2026년 파주시 SNS 운영 용역	점검일	2026. 8. 31.
개인정보 보호책임자 (수탁자)	한선영 (서명)	점검자	한선영 

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 임무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	○	

15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	○	
16	악성프로그램 경보가 발생되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	○	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	○	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	○	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단탐지 등 안전조치를 하고 있는가?	○	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	○	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	○	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	○	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 알고리즘으로 암호화하여 저장하고 있는가?	○	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	○	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	○	

세외수입 체납안내문 제작 용역

[붙임10]

수탁업체 개인정보 관리 실태 점검표

수탁기관명	(주) 조두니	점검기간	2026. 9. 2. 09:50 ~ 11:00
사업명	세외수입 제정안(안) 제정	점검일	2026. 9. 2.
개인정보 보호책임자 (수탁자)	김성민	점검자	김지민 AI정책팀 이정민 기획팀

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	해당없음	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	해당없음	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	해당없음	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	해당없음	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	해당없음	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	해당없음	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	해당없음	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	해당없음	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	해당없음	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	○	

15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	○	
16	악성프로그램 경보가 발생되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	○	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	개인정보취급자	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	○	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단·탐지 등 안전조치를 하고 있는가?	개인정보취급자	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	개인정보취급자	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	개인정보취급자	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	○	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	개인정보취급자	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	개인정보취급자	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 알고리즘으로 암호화하여 저장하고 있는가?	○	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	개인정보취급자	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	○	

2026년 체납차량 번호판영치 프로그램 및 영치장비 유지보수

수탁업체 개인정보 관리 실태 점검표

부서명	사무과	점검기간	2026년
사업명	번호판영치프로그램 및 영치장비유지보수	점검일	2026. 8. 28. (목)
용역책임자(사업자)	한지현 (서명) 	점검자	주영민 (서명) 

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	채 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	-	해당항목 미검
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위도 사들 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	-	해당항목 미검

무보험자동차 송치관리시스템

수탁업체 개인정보 관리 실태 점검표

부서명	차량등록사업소	점검기간	2026.1.1. ~ 2026.8.26.
사업명	가.무보험시스템 유지관리 나.무단방치시스템 유지관리	점검일	2026.8.26.
개인정보 보호책임자 (수탁자)	선우정보 정종보	점검자	손성호

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	제 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	

14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	☐	
15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	☐	
16	악성프로그램 경보가 발생되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	☐	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	☐	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	☐	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단 탐지 등 안전조치를 하고 있는가?	☐	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	☐	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	☐	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	☐	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	☐	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	☐	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	☐	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	☐	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장 매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	☐	

파주시 도시정보센터 통합관제시스템 유지관리

[붙임10]

수탁업체 개인정보 관리 실태 점검표

수탁기관명	(주) 베이스	점검기간	2026. 8. 1 13:00 ~ 14:00
사업명	파주시도시정보센터 통합관제시스템 유지관리	점검일	2026. 9. 1
개인정보 보호책임자 (수탁자)	안승민	점검자	이정민 (수탁자)

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	내부관리
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	○	

15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	0	
16	악성프로그램 경보가 발생되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	0	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	0	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	0	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단·탐지 등 안전조치를 하고 있는가?	0	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	개인망	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	0	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	0	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	0	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	0	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 알고리즘으로 암호화하여 저장하고 있는가?	0	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	X	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	0	

2026년 영구지적기록물 전산화사업

수탁업체 개인정보 관리 실태 점검표

부서명	토지정보과	점검기간	2026.3.16. ~
사업명	영구지적기록물 전산화용역	점검일	2026.5.8.
용역책임자(사업자)	김수진 (서행준)	점검자	유희곤 (유현문)

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	x	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	x	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일	○	

	기기에 조치를 하고 있는가?		
15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	○	
16	악성프로그램 경보가 발령되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	○	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	○	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	○	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단탐지 등 안전조치를 하고 있는가?	○	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	○	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	○	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	○	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	○	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?		해당없음
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장 매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?		해당없음

복무관리 및 무인경비시스템 유지보수

[별지 제5호 서식] 개인정보위탁사업 자체점검표

개인정보 위탁사업 점검표

위탁 사업명	업체명	점검일	점검자	
			직급	성명
복무관리 및 무인경비 시스템 유지보수	(주)에스원	25. 12. 31.	지방행정서기	고안나 (서명)

점검항목		예	아니오	해당 없음	기타
1.	개인정보처리업무 위탁계약서 작성	○			
2.	위탁계약서 표준 개인정보처리 위탁 계약서 준용 작성여부	○			표준 계약서 준용 작성
3.	보안서약서 제출여부	○			
4.	개인정보 교육실적	○			교육 실시 실적
5. 양식 비치 현황	파기대장 (자료 전달 시)			○	
	보조기억매체 반출입대장			○	
	동제구역 출입대장			○	
6. 자료	자료 제공/열람 대장			○	
	보관상태 양호여부			○	
7. 파기	사용기간 경과 자료 파기여부			○	
	출력물 파기상태			○	
8	재 위탁 여부		○		
9.	위탁업무 수행 목적 외 개인영상정보 처리 여부			○	
10.	계약 종료 후 사후관리	수탁자 계정·권한 말소 등 접근권한 관리		○	

자동차세 고지서 제작

[붙임10]

수탁업체 개인정보 관리 실태 점검표

수탁기관명	삼부전산	점검기간	2026. 9. 1. (14:15 ~ 15:10)
사업명	2026 자동차세 고지서 제작	점검일	2026. 9. 1.
개인정보 보호책임자 (수탁자)	장 인혁 (서명)	점검자	AI 정해민 이정민 (서명)

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	○	
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	○	

15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	○	
16	악성프로그램 경보가 발생되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	○	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	○	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	○	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단·탐지 등 안전조치를 하고 있는가?	○	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	해당없음	
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	○	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	○	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	○	
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	○	
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	○	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	○	

번호판영치시스템 유지보수

수탁업체 개인정보 관리 실태 점검표

부서명	파주시 차량등록사업소	점검기간	2026. 1 ~ 8
사업명	2026년도 번호판 영치시스템 프로그램 유지보수 계약	점검일	8 - 28
개인정보 보호책임자 (수탁자)	(주)제이컴모빌피아 이준호	점검자	정옥순

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?	○	
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?	○	
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?	○	
4	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?	-	삭제함
5	내부 관리계획의 수립·시행하고 있으며, 이행 실태를 연1회 이상 점검·관리 하고 있는가?	○	
6	개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하고 있는가?	○	
7	개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하고 있는가?	○	
8	개인정보처리시스템 접근 권한의 부여·변경·말소 내역을 기록하고 그 기록을 최소 3년간 보관하고 있는가?	○	
9	개인정보취급자의 개인정보처리시스템 접속기록을 1년 이상(단, 5만명 이상 정보주체의 개인정보, 또는 고유식별정보나 민감정보를 처리하는 경우에는 2년 이상) 보관·관리 하고 있는가?	○	
10	개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 접속기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 모두 포함하고 있는가?	○	
11	개인정보취급자의 개인정보처리시스템 접속기록 등을 월1회 이상 점검하고 있는가?	○	
12	개인정보처리시스템 접속기록 점검 시 개인정보 다운로드가 발견되는 경우, 내부 관리계획 등에서 정한 바에 따라 그 사유를 확인하고 있는가?	○	
13	개인정보취급자의 개인정보처리시스템 접속기록을 안전하게 보관하고 있는가?	○	
14	처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기에 조치를 하고 있는가?	-	확인함

15	업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램(백신 소프트웨어 등)을 설치·운영하고, 보안 프로그램의 자동 업데이트 기능을 사용하거나 정당한 사유가 없는 한 일 1회 이상 업데이트하여 최신 상태로 유지하고 있는가?	0	
16	악성프로그램 경보가 발생되거나, 응용 프로그램이나 운영체제 소프트웨어의 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 업데이트를 실시하고 있는가?	0	
17	개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 있는가?	0	
18	개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?	0	
19	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 침입차단·탐지 등 안전조치를 하고 있는가?	0	
20	개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 또는 가상사설망 등 안전한 접속수단을 적용하고 있는가?	-	정보통신망
21	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접속할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?	0	
22	개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 시스템 접속이 차단되도록 하는 등 조치하고 있는가?	0	
23	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 정보통신망을 통하여 송·수신하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	0	
24	개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하고 있는가?	-	정보통신망
25	고유식별정보를 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ), 내부망에 저장하는 경우, 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	-	정보통신망
26	비밀번호, 생체인식정보, 전자서명값, 인증토큰 등 인증정보를 저장하는 경우 이를 안전한 암호 알고리즘으로 암호화하고 있으며, 비밀번호의 경우 복호화되지 아니하도록 일방향 암호화하여 저장하고 있는가?	0	
27	고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘으로 암호화하여 저장하고 있는가?	-	정보통신망