

수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 정보화장비 유지관리

○ 수탁사명 : 주식회사 디에스티 ○ 점검일 : '25. 3. 19.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	O		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	O		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	O		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제에의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	O		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	O		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	O		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	O		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	O		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	O		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	O		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	O		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	6		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	○		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	○		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	○		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	○		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	○		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	○		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	○		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		○		

※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인

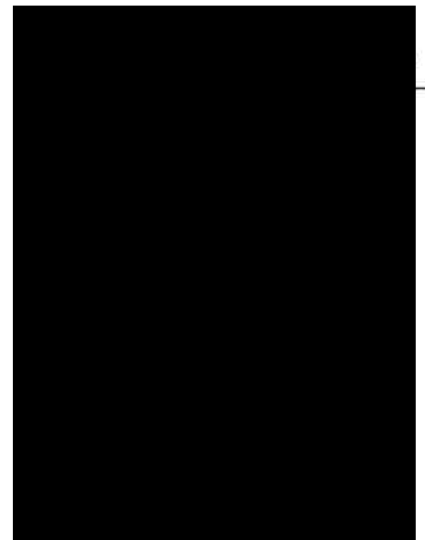
부서 : 디베스티

직책 : 부장

○ 관리부서 확인

부서 : 사립대학내 개인정보

직책 : 국무행정관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : _____ 정보시스템 유지관리 _____

○ 수탁사명 : _____ 낙스넷(주) _____

○ 점검일 : _____ '25. 3. 19. _____

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	✓		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	✓		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	✓		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제에의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	✓		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	✓		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	✓		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	✓		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	✓		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	✓		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	✓		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	✓		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	✓		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	✓		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	✓		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	✓		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	✓		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	✓		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	✓		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	✓		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		✓		

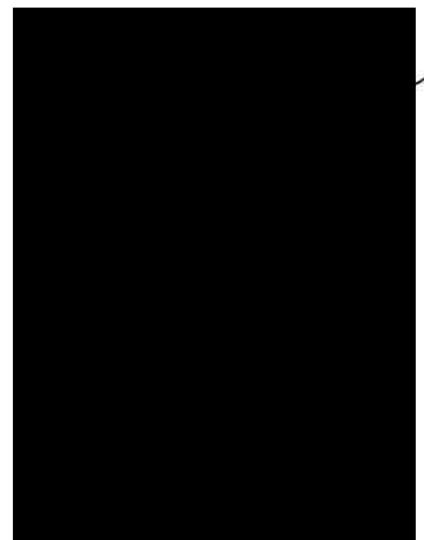
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : 유티관리팀 직책 : 부장

○ 관리부서 확인 부서 : 사랑내향디지털지원부 직책 : 극복해장관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 폐교대학 통합관리시스템 운영·유지관리
 ○ 수탁사명 : (주)퓨전소프트 ○ 점검일 : '25. 3. 19.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	✓		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	✓		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	✓		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제에의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	✓		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	✓		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	✓		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	✓		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	✓		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	✓		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	✓		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	✓		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	✓		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	√		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	√		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	√		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	√		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	√		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련 하고 정기적으로 점검 여부	√		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	√		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		√		

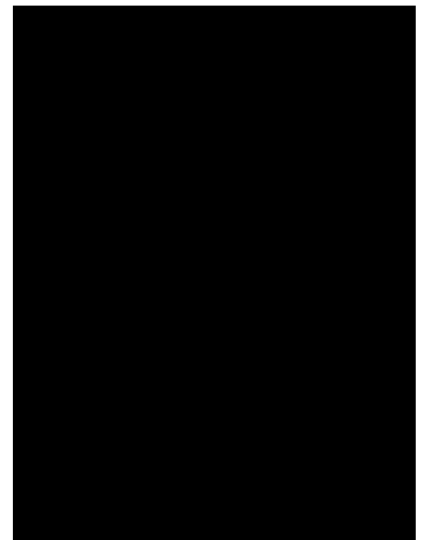
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : 개발팀 직책 : 책임

○ 관리부서 확인 부서 : 사감악디거턴관 직책 : 주무행정관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 대학정보화시스템(u-erp) 유지관리
 ○ 수탁사명 : (주)신라시스템 ○ 점검일 : '25. 3. 19.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	0		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	0		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	0		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제에 관한 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	0		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	0		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	0		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	0		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	0		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	0		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	0		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	0		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	0		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	○		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	○		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	○		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	○		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	○		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	○		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	○		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		○		

※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인

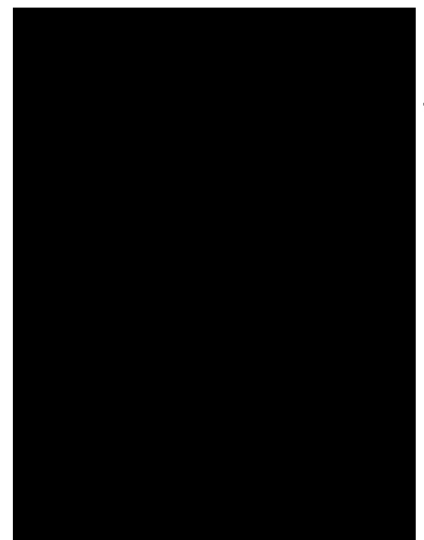
부서 : 선라시스템

직책 : 수석

○ 관리부서 확인

부서 : 시정대안지원지원부

직책 : 국무행정관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 대학재정정보시스템(기본재산 및 기채 사후관리) 고도화
 ○ 수탁사명 : 신라시스템 ○ 점검일 : '25. 3. 19.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	○		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	○		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	○		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	○		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	○		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	○		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	○		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	○		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	○		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	○		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	○		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	○		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	<input type="radio"/>		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	<input type="radio"/>		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	<input type="radio"/>		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	<input type="radio"/>		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	<input type="radio"/>		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련 하고 정기적으로 점검 여부	<input type="radio"/>		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	<input type="radio"/>		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		<input type="radio"/>		

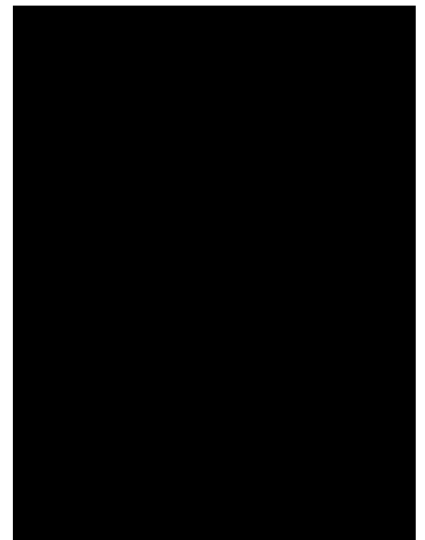
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : SI사업부 직책 : 상무이사

○ 관리부서 확인 부서 : *사립대학디지털교육실* 직책 : *교육행정실장*



점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	○		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	○		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	○		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	○		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	○		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	○		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	○		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		○		

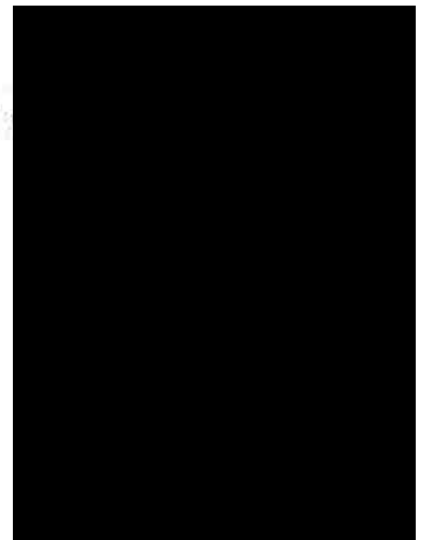
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : DST 직책 : 부장

○ 관리부서 확인 부서 : 사람대우 디지털개혁 직책 : 국무행정관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 정보시스템 유지관리

○ 수탁사명 : 낙스넷(주)

○ 점검일 : '25. 2. 19.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	✓		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	✓		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	✓		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	✓		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	✓		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	✓		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	✓		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	✓		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	✓		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	✓		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	✓		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	✓		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	✓		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	✓		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	✓		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	✓		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	✓		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	✓		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	✓		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		✓		

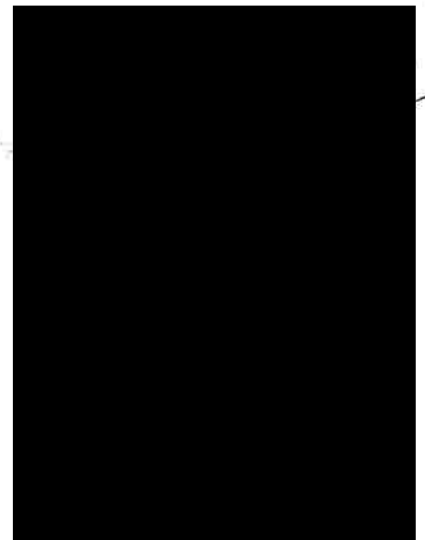
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : 유지관리팀 직책 : 부장

○ 관리부서 확인 부서 : 사민내선대리팀장 직책 : 국록행정관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 폐교대학 통합관리시스템 운영·유지관리
 ○ 수탁사명 : (주)퓨전소프트 ○ 점검일 : '25. 2. 19.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	✓		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	✓		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	✓		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	✓		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	✓		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	✓		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	✓		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	✓		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	✓		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	✓		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	✓		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	✓		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	✓		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	✓		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	✓		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	✓		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	✓		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련 하고 정기적으로 점검 여부	✓		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	✓		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		✓		

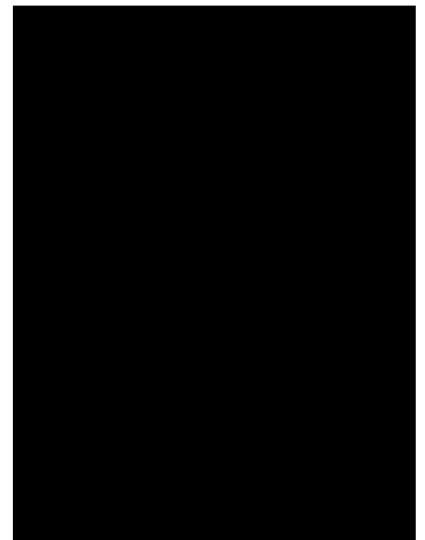
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : 개발팀 직책 : 책임

○ 관리부서 확인 부서 : 사람데이터센터개발 직책 : 국복임정간



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 대학정보화시스템(u-erp) 유지관리
 ○ 수탁사명 : (주)신라시스템 ○ 점검일 : '25. 2. 19.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	o		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	o		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	o		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제에의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	o		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	o		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	o		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	o		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	o		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	o		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	o		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	o		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	o		

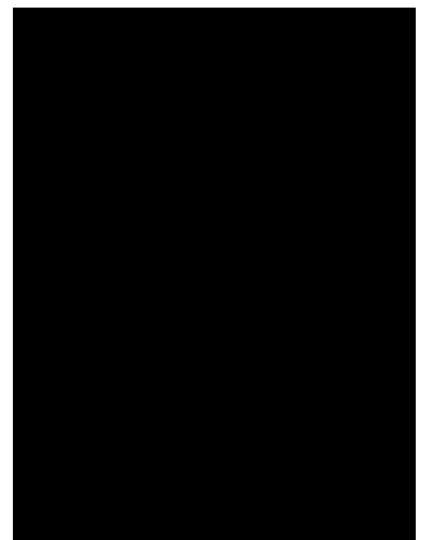
점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	○		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	○		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	○		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	○		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	○		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	○		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	○		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부				○

※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

- 수탁사 확인 부서 : 신라시스템 직책 : 수석
- 관리부서 확인 부서 : 자랑 대각 디제이티브 직책 : 주요임원



점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	✓		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	✓		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	✓		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	✓		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	✓		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	✓		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	✓		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부				✓

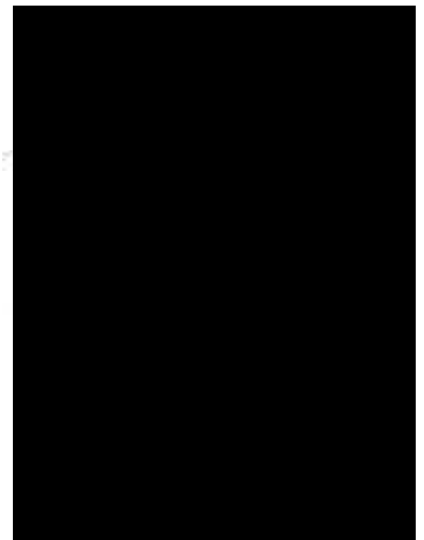
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : 사업관리 직책 : 대표

○ 관리부서 확인 부서 : *사립대학 디지털개발* 직책 : *주목래장관*



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 대학재정정보시스템(기본재산 및 기채 사후관리) 고도화

○ 수탁사명 : 신라시스템 ○ 점검일 : '25. 2. 19.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	○		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	○		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	○		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	○		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	○		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	○		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	○		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	○		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	○		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	○		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	○		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	○		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	○		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	○		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	○		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	○		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	○		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련 하고 정기적으로 점검 여부	○		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	○		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		○		

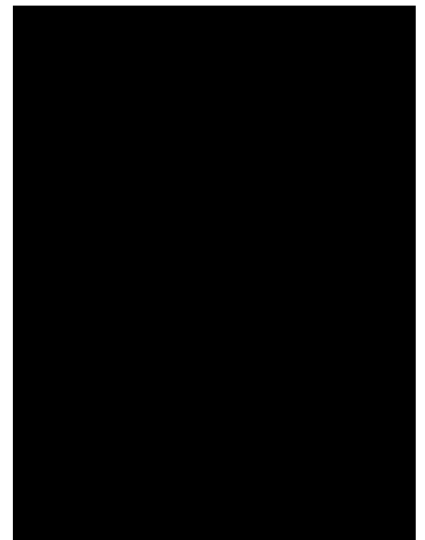
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : SI사업부 직책 : 상무이사

○ 관리부서 확인 부서 : 사립대학디지털대학 직책 : 국학영장관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 정보화장비 유지관리

○ 수탁사명 : 주식회사 디에스티

○ 점검일 : '25. 1. 15.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	○		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	○		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	○		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	○		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	○		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	○		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	○		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	○		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	○		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	○		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	○		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	○		

점검 항목		예	아니오	해당없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	○		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	○		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	○		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	○		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	○		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	○		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	○		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		○		

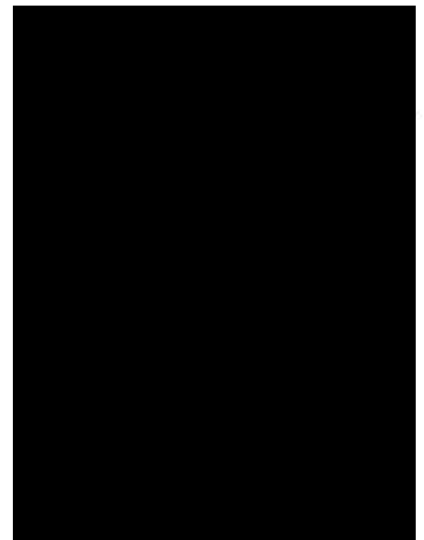
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : DST 직책 : 목장

○ 관리부서 확인 부서 : 사립대학디지털교육 직책 : 극동행정관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 정보시스템 유지관리

○ 수탁사명 : 낙스넷(주)

○ 점검일 : '25. 1. 15.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	✓		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	✓		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	✓		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	✓		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	✓		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	✓		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	✓		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	✓		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	✓		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	✓		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	✓		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	✓		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	✓		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	✓		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	✓		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	✓		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	✓		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련 하고 정기적으로 점검 여부	✓		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	✓		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		✓		

※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : 유지관리팀 직책 : 부장

○ 관리부서 확인 부서 : A팀/내각/디지털정책 직책 : 직무책임자



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 폐교대학 통합관리시스템 운영·유지관리
 ○ 수탁사명 : (주)퓨전소프트 ○ 점검일 : '25. 1. 15.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	✓		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	✓		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	✓		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	✓		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	✓		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	✓		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	✓		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	✓		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	✓		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	✓		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	✓		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	✓		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	√		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	√		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	√		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	√		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	√		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	√		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	√		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		√		

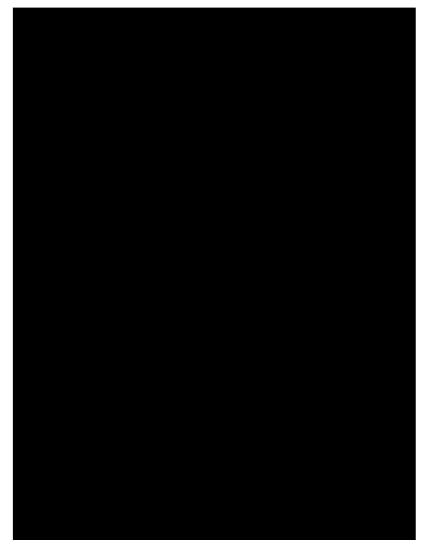
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : 개발팀 직책 : 책임

○ 관리부서 확인 부서 : 행정대안디지털 직책 : 주무관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 대학정보화시스템(u-erp) 유지관리
 ○ 수탁사명 : (주)신라시스템 ○ 점검일 : '25. 1. 15.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	9		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	0		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	9		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	9		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	0		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	9		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	9		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	9		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	0		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	9		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	0		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	0		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	4		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	4		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	4		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	0		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	0		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검 여부	4		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	4		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부				0

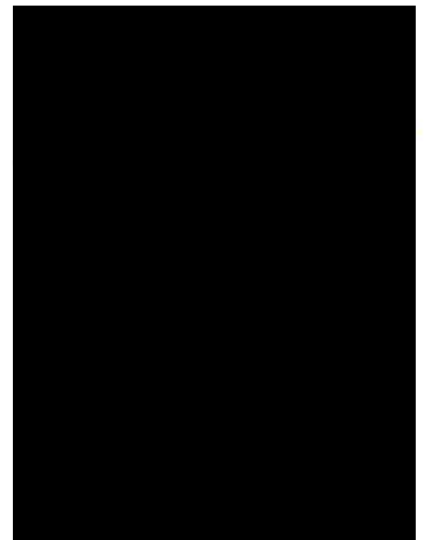
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : 신라시스템 직책 : 부장

○ 관리부서 확인 부서 : 사랑내보내기연구소 직책 : 극복재정리관



점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	✓		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	✓		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	✓		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	✓		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	✓		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련 하고 정기적으로 점검 여부	✓		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	✓		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부				✓

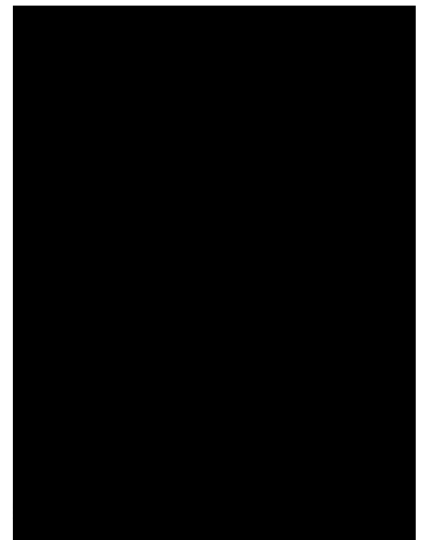
※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : 사업관리 직책 : 대표

○ 관리부서 확인 부서 : 사람관리비서관 직책 : 국무행정관



수탁자 개인정보보호 관리실태 점검표

○ 사업명 : 대학재정정보시스템(기본재산 및 기채 사후관리) 고도화
 ○ 수탁사명 : 신라시스템 ○ 점검일 : '25. 1. 15.

점검 항목		예	아니오	해당 없음
1. 개인정보 취급자의 역할 및 책임에 관한 조치 여부	1-1. 개인정보 취급자에 대한 보약서약서 제출 등 관리 여부	0		
	1-2. 개인정보 취급자에 대한 교육 실시 여부	0		
	1-3. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 여부	0		
2. 개인정보에 대한 접근 권한 제한 및 접근 통제에의 조치 여부	2-1. 개인정보 처리시스템에 대한 접근권한 차등 여부	0		
	2-2. 침입차단·탐지 시스템 및 개인정보 처리 시스템의 설치 및 운영 여부	0		
	2-3. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 여부	0		
	2-4. 비인가된 P2P, 웹하드, 공유 설정에 대한 차단 여부	0		
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 여부	3-1. 비밀번호의 일방향 암호화 저장 등 인증 정보의 암호화 저장 여부	0		
	3-2. 주민등록번호 등 고유식별정보의 암호화 저장 여부	0		
	3-3. 정보주체의 개인정보 또는 인증정보를 송·수신하는 경우 암호화 여부	0		
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 여부	4-1. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 여부	0		
	4-2. 개인정보처리시스템 접속기록의 위·변조 및 도난, 분실되지 않도록 안전한 관리 (보관) 및 취약점 점검 여부	0		

점검 항목		예	아니오	해당 없음
5. 개인정보에 대한 보안프로그램의 설치 및 보안 갱신 조치 여부	5-1. 보안프로그램 설치 및 정기적 업데이트 수행 여부	○		
	5-2. 악성프로그램 감염 방지 등을 위한 보안조치 적용 여부	○		
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 여부	6-1. 개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부	○		
	6-2. 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책 이행 여부	○		
	6-3. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 이행 여부	○		
7. 위험 분석 및 관리에 관한 조치 여부	7-1. 위기대응 매뉴얼 등 대응 절차를 마련 하고 정기적으로 점검 여부	○		
	7-2. 개인정보 처리시스템 백업 및 복구를 위한 계획 마련 여부	○		
8. 개인정보 보유기간의 경과 및 목적 달성 등의 불필요하게 되었을 시 파기 여부		○		

※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ 각 점검항목에 대한 점검결과에 대한 근거 자료를 첨부함

※ "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기를 말함

○ 수탁사 확인 부서 : SI사업부 직책 : 상무이사

○ 관리부서 확인 부서 : *서강대학교디지털교육* 직책 : *극복생장관*

