오라클 DB 칼럼 암호화 솔루션 도입 사업

제안요청서

2026. 9.

동양미래대학교

종합정보지원실

Ⅰ 사업 개요

1. 개요

가. 사업명: 오라클 DB 칼럼 암호화 솔루션 도입 사업

나. 사업 예산: 금 60,000,000원 (부가세 포함)

다. 사업 기간: 계약일 ~ 2026. 12. 31. (목)

라. 입찰 및 계약 방법: 2단계 경쟁입찰

2. 사업 목적

가. 개인정보보호법 준수: 고유식별정보, 바이오정보, 인증 정보 암호화 저장 의무 이행

나. 데이터 유출 시 피해 극소화: 데이터 유출시에 별도 저장된 복호화키로 복호화 불가

다. 내부자에 의한 무단 접근 및 남용 방지: 데이터베이스관리자, 인프라 담당자 등 직무와 관련없는 내부자의 정보 열람 차단

3. 사업 목표

가. 암호화 모듈과 암복호화 키의 물리적인 분리

나. 최신 암호화 적용에 능동적으로 대응할 수 있는 암호화 모듈 도입

다. 추가 암복호화 키를 통합하여 관리할 수 있는 암복호화 키관리 모듈 도입

라. 암복호화 키 백업 및 복구의 용이성으로 장애시 신속한 대응 가능

4. 사업 범위

가. DB 칼럼 암호화 솔루션 도입
- 오라클 운영 DB: 16Core x 2대 (이중화, HA)
- 오라클 개발 DB: 16Core x 1대

나. DB 칼럼 암호화 키 관리 솔루션 도입

다. 기존 암호화 데이터의 안전한 재암호화

라. 업무 애플리케이션 영향도를 최소화하는 무수정(Zero-code Change) 암복호화 모듈 교체

5. 기대 효과

가. 개인정보 보호법 시행령 제30조 및 안전성 확보조치 기준에 명시된 필수 암호화 대상(주민등록번호, 비밀번호, 계좌번호 등)에 대한 법적 의무 이행

나. 암호 키 분리 보관으로 데이터 탈취시에도 암호화된 데이터의 평문 노출 예방하여 대학의 신뢰 유지

다. 칼럼 암호화 환경 기반 마련으로 추가적인 암호화 대상 칼럼 확장이 용이

Ⅱ 제안 요청 내용

1. 제안 요청 개요

가. 본 내용은 본 사업과 관련된 모든 세부사업에 대하여 공통으로 적용함

나. 모든 제안 내용은 대학이 제시한 조건에 충족하여야 하며, 주사업자가 일괄 제안해야 함

다. 본 제안요청서에 명시된 모든 조항은 대학이 요구하는 최소한의 사항만이 규정되었으므로, 상세하게 기술되지 않았거나 누락된 사항에 대해서도 본 사업의 목적과 내용에 명시된 목표시스템 구현에 전혀 문제가 발생하지 않도록 제안업체는 철저히 검토하여 반드시 사전조치를 강구하고 대학과 협의하여 실제 구현 및 설치등에 명확히 반영하여야 함

라. 개발에 사용된 모든 인프라(H/W, S/W, 이미지, 폰트 등)는 저작권에 문제가 없어야 하며, 비용이 발생할 경우 주사업자가 부담하여야 함

마. 프로젝트 개발 중에 제안요청서, 제안서 등의 내용이 상이할 경우 발주기관의 해석을 따라야 함

2. 시스템 구성 요구사항

가. 암호화 솔루션 제품명: D'Amo (제조사: Pentasecurity)

나. 암복호화 모듈 도입

1) 대상
   - 오라클 운영 DB: 16Core x 2대 (이중화/HA)
   - 오라클 개발 DB: 16Core x 1대

2) 현행 운영 중인 서비스 애플리케이션의 소스 코드 수정없이 적용 가능한 DB 컬럼 암호화 방식 제한

3) 기존 암복호화 모듈의 호출 방식을 그대로 지원하여 업무 연속성 및 개발 공수 최적화

나. 암복호화 키 관리 모듈 도입

1) 암복호화 모듈 및 키 관리 기능을 물리적으로 분리된 구조로 구축

2) 시스템 확장, 신규 데이터 암호화 추가 발생 시, 생성·폐기·주기적 갱신 등 전체 라이프사이클에 걸쳐 다양한 암복호화 키를 통합 관리·운영

3) 이종 시스템 및 복수의 DB 환경으로 암호화 대상이 확대되더라도 중앙 키 관리 시스템(KMS)을 통해 정책 및 키를 일관성 있게 제어할 수 있는 아키텍처 제시

다. 관리자 웹 콘솔 기능

1) 관리자 웹 콘솔 접속 시 허용된 IP 주소에서만 등록 및 접속을 허용하는 접근 제어 기능을 제공해야 하며, 비인가 IP에서의 접속 시도를 실시간으로 차단하고 감사 로그 기록

2) 관리자 계정의 보안 강화를 위해 설정된 일정 주기에 따라 비밀번호 변경을 강제하고, 비밀번호 복잡도 요건(영문, 숫자, 특수문자 조합 등) 및 이력 관리를 통한 기존 비밀번호 재사용 금지 기능 제공

3) 연속 로그인 실패 횟수 및 계정 잠금 유지 시간을 관리자가 자유롭게 설정

4) 로그인 실패로 잠긴 계정은 지정된 잠금 시간이 경과한 후 자동 해제되거나, 최고 관리자 권한을 통한 수동 임시 잠금 해제 기능 제공

5) 임계치 초과 로그인 실패 발생 시 해당 접속 시도 정보(IP, 시각, 시도 계정 등)를 감사 로그로 보관하고, 관리자에게 즉시 알림 발송

3. 데이터 요구사항

가. 기존 암호화된 데이터의 신규 키/알고리즘 기반으로 재암호화 하기 위한 마이그레이션 절차서 작성 및 전담 기술 지원 인력 투입

나. 제안사는 대학과 함께 기존 암호화 데이터를 복호화 한 후, 재암호화 테스트를 수행하여 원본 데이터와의 정합성 및 무결성 입증

4. 성능 요구사항

가. 데이터 재암호화 시 수행 시간 단축을 위한 기술적 지원 제공

나. 특정 시점에 트래픽 집중시에도 안정적인 암복호화 처리 성능 유지

5. 테스트 요구사항

가. 기존 암호화되어 있는 데이터 이관에 대한 테스트를 통한 마이그레이션 방안 제공

1) 데이터 마이그레이션 시 총 소요 시간(RTO) 측정 지원

2) 모의 테스트 중 장애 발생 상황을 가상하여 기존 데이터로의 즉시 복구(Rollback) 절차 및 서비스 연속성 확보 방안 제시

6. 보안 요구사항

가. 사업 수행 중 대학의 「보안업무」관련 법 및 규정에 따라 사업 수행

나. 본 사업의 참여 인력은 신원이 확실한 자로 구성하여야 하며, 보안사고에 대한 책임은 사업자가 부담

다. 사업 착수, 수행, 완료 등 사업 전체 단계별 보안 관리 방안 수립

1) 사업 수행에 필요한 인원, 문서, 장비 등의 보안관리 계획을 수립하여야 하며, 보안상 결격 사항이 없도록 조치

2) 사업기간 내 보안 문제 발견 시, 즉시 그 대책을 수립하고 해결 방안을 제출

라. 【붙임1】의 【별지2】 사업자 보안 위규 처리기준을 숙지하고, 사업을 수행하여야 하며, 보안 위규 사항 발생 시에는 【붙임1】의 【별지4】의 보안위약금 부과 기준에 의해 위약금 배상

마. 【붙임1】의 부정당업자 제재대상이 되는 【별지1】 누출금지정보가 누출 시, 해당 업체를 부정당업자로 등록하고 「지방자치단체를 당사자로 하는 계약에 관한 법률 시행령」 제92조에 따라 부정당업자로 등록 및 입찰 참가자격 제한 등 제재 조치

바. 본 계약과 관련하여 취득한 비밀 사항을 계약 기간 및 종료 후에도 제3자에게 누설하여서는 아니되며, 누설하였을 경우 이에 따른 민·형사상의 책임을 짐

사. 투입인력에 대한 보안통제

1) 용역사업 참여인원은 업체 임의로 교체할 수 없으며, 변동사항 발생 즉시 보고

2) 보안책임자 직무·역할

- 사업수행자는 보안사항의 도난, 분실 등 제반 보안사항의 조치, 보안책임자를 지정·운영
- 보안상 중요하다고 생각되는 모든 기록과 자료는 시건장치가 되어있는 곳에 보관하고, 보안담당자는 이를 관리

7. 제약사항

가. 하도급 관련 법령 준수

1) 본 사업과 관련하여 제3의 업체에게 일괄 하도급을 할 수 없으며, 기술특성상 하도급이 필요한 경우「소프트웨어 진흥법」제51조, 같은법 시행규칙 제14조에 따라 사전 승인을 받아야 함

- 인력 중 주관 공급사 또는 공동수급인 경우 공동수급자 소속 이외의 인력은 하도급으로 간주

2) 하도급은「소프트웨어 진흥법」제51조의 제1항에 따라 사업금액의 100분의 50을 초과할 수 없으며, 제2항에 따라 재하도급은 원칙적으로 불허함

나. 보상 요건 및 저작권 준수 등

1) 본 유지관리 사업을 위해 공급하는 모든 물품 및 S/W는 신품 또는 정품이어야 하며 관련 저작권법에 의해 저작권자의 권익을 침해하지 않아야 함

2) 사업수행자는 당해 사업 수행하는 과정에서 용역목적물 및 제3자에 대한 손해를 발생시킨 경우, 그 손해를 부담함

3) 본 사업은 개발의 기여도 및 계약목적물의 특수성(보안, 영업비밀 등)으로, 수행결과물(계약 목적물)에 대한 지식재산권은 발주기관에게 있음

8. 프로젝트 관리 요구사항

가. 산출물 및 제출 서류

주체 구분	산출물 및 제출 서류	제출 시기	비고
대표자	- 사업시작시 보안확약서(대표자용)	사업 시작 시	【붙임2】
	- 사업종료시 보안확약서(대표자용)	사업 종료일	【붙임3】
사업책임자	- 보안서약서 - 원격접속 보안서약서 - 개인정보보호 관련 교육 이수증(2026년도)	사업 시작 시	【붙임4】 【붙임5】 -
	- 수탁업체 개인정보보호 현황 점검표	계약 시	
	- 완료보고서: 개인정보영향평가 및 정보보호수준 진단 증빙에 적합한 내용을 포함해야 함	사업 종료 2주 전	
	- 운영 매뉴얼(구성도, 관리자 기능 등)	사업 종료일	
	- 개인정보파기 확인서	사업 종료일	
사업참여자	- 보안서약서 - 원격접속 보안서약서 - 개인정보보호 관련 교육 이수증(2026년도)	사업 시작 시	【붙임4】 【붙임5】 -
	- 개인정보파기 확인서	사업 종료일	

나. 위험관리

1) 위험관리계획 수립 및 이행

- 위험관리계획을 수립하여 계약기간동안 발생할 수 있는 위험식별, 정성적·정량적 분석, 대응계획, 감시, 통제 등을 수행함 (예상위험 : 인력수급, 요구사항 변경, 기술적 취약점 등)

2) 위험 대응계획수립 및 조치

- 식별된 위험 및 이슈사항에 대해서는 위험관리대장에 등재하고, 사전 위험 및 사후위험 관리를 수행함
- 위험관리대장 내 위험 및 이슈사항에 대해서는 발주기관에 보고하고, 분석 및 대응계획, 감시·통제사항을 보고함

Ⅲ 제안서 작성 안내

1. 일반사항

가. 제안사는 제안요청서의 내용을 충분히 확인 및 인지한 후 제안하여야 함

나. 제출된 제안서 및 관련 자료는 반환하지 않으며, 공개하지 않음

다. 제안서의 내용이 허위 또는 이행 불가능한 내용으로 작성된 사실이 발견되었을 경우 제안업체에서 일체의 책임을 짐

라. 제안서 내용에 대한 증빙자료는 페이지 수의 제한을 받지 않고 별첨으로 제출 가능

2. 제안 자격 요건

가. 국가를 당사자로 하는 계약에 관한 법률 시행령 제12조 및 동법 시행규칙 제14조에 정한 자격을 갖춘 업체

나. 국가를 당사자로 하는 계약에 관한 법률 제27조 및 동법 시행령 제76조에 따라 부정당업자에 해당하지 않는 업체

다. 입찰공고일 기준「소프트웨어 진흥법」제58조 및 같은 법 시행규칙 제17조에 따라 소프트웨어사업자 일반현황 관리확인서를 발급받아 제출할 수 있는 업체

라. 입찰공고일 기준 부정당업자로 지정되지 아니한 업체이어야 하며, 현재 부도, 파산, 및 금융 신용부실로 정상적인 영업활동에 지장이 없는 업체

마. 입찰공고일 현재 국세 및 지방세 체납사실이 없는 업체

바. **“제조사 공급 및 기술지원 확약서” 제출이 가능한 업체**

- **제품명**: D’Amo (**제조사**: Pentasecurity)

3. 제안서 신청

가. 서류제출

1) 본 사업의 제안에 참여하고자 하는 업체는 반드시 제안서 제출기한 마감 전에 지정장소에 필요한 모든 서류를 제출하여야 함

2) 제출기한을 초과하거나 제안참가를 위한 서류가 누락된 경우 제안참가 신청을 무효로 함

3) 제안서는 제출서류를 구비하고 대표자의 인감(또는 사용인감)을 날인하여 직접 제출하여야 함(우편접수는 인정하지 않음)

나. 제출기한 및 장소: 입찰공고 참조

다. 제출서류

1) 제안서 제출

- 제안서 및 발표자료 10부

(제안서분량: 100페이지 이내, 발표자료분량: 20페이지 이내)

- 제안서가 수록된 USB 1매

2) 기타 입찰관련 서류 제출: 입찰공고 참조

라. 제안서 관련 문의처: 입찰공고 참조

4. 제안서 작성 시 주의사항

가. 제안서는 허위 또는 예상으로 작성하지 않아야 하며, 모든 기재사항은 객관적으로 입증할 수 있어야 하고, 허위로 작성한 사실이 발견될 때에는 평가에서 제외하며 계약체결 이후인 경우에는 당해계약을 해제 또는 해지할 수 있음

나. 제안서의 내용이 요구사항을 충족치 못하거나 규격에 어긋난 경우 평가 대상에서 제외함

다. 접수된 제안서의 내용은 본교의 승인 없이 변경(수정, 추가, 삭제)할 수 없으며, 계약체결 시 계약조건으로 간주함

라. 본 제안요청서와 제안 참가자의 제안서는 계약서의 일부가 되고, 본교는 필요시 제안 참가자에게 추가제안이나 추가 자료를 요청할 수 있으며, 이에 따라 제출된 자료는 제안서와 동일한 효력을 가짐

마. 지식재산권 및 소유권 보호를 위하여 본 사업수행으로 인해 발생되는 모든 유.무형의 성과물은 본교의 소유로 귀속됨

바. 제안서의 내용은 제안사가 수행업체로 선정된 후 계약서에 명시되지 않더라도 계약서와 동일한 효력을 가지며, 계약서에 명시된 경우는 계약서를 우선함

사. 제안서 외에 제출되는 서류는 본교의 양식으로 제출하는 것을 원칙으로 하며, 원본이 존재할 경우에는 반드시 원본대조필을 서명하고, 원본은 별도로 제출함

아. 본 제안과 관련된 일체의 소요비용은 제안업체의 부담임

자. 기타 언급되지 않은 사항은 본교의 제반 규정에 따름

Ⅳ 사업자 선정

1. 입찰 방식

가. 입찰방식: 2단계 경쟁입찰

나. 업체평가 및 선정 방법

1) 내부 규정에 따라 정보화추진위원회에서 입찰 참가업체가 제안한 제안서 발표 내용을 종합적으로 평가하고 평가한 점수를 평균하여 기술평가점수를 산출

2) 제안서 발표에 참가하지 않는 업체는 기술평가대상에서 제외

3) 기술평가점수 만점의 85% 이상 획득한 업체를 대상으로 기술적격자로 선정

4) 기술적격자로 선정된 업체에 한하여 가격입찰서 개찰

5) 예정가격 이하로서 최저가격을 제시한 업체를 낙찰자로 선정

6) 기타 제안요청서에 명시되지 않는 사항은 계약 관련 규정 및 법령에 따름

다. 유의사항

1) 제안서 제출업체는 심사 결과에 대하여 일체의 이의를 제기할 수 없으며, 평가 결과는 공개하지 않음

2) 제안서가 부실하거나 입증자료가 불확실한 경우 또는 기준 미달인 경우에는 원칙적으로 평가 대상에서 제외함

3) 평가결과에 대해서는 일체 공개하지 않으며 이의를 제기할 수 없음

4) 제안서에 기재된 내용 이외의 자료는 평가대상에서 제외함

5) 제안 내용은 꼭 필요한 사항 위주로 간단명료하게 작성되어야 하며, 내용 중 "~할 수도 있다", "~을 고려하고 있다" 등의 애매모호한 표현은 구축할 수 없는 것으로 간주함

6) 제안내용의 전부 또는 일부에 대하여 담합한 사실이 발견되거나 담합하였다고 판단되는 경우 제안을 무효로 함

7) 제안요청서에 누락된 업무 또는 제안서에 제시하지 않은 업무도 사업 시행 시 학교의 요청에 따라 사업 시행사와 협의 후 변경 조정할 수 있음

2. 평가 기준

가. 기술 평가표

평가 구분	평가 항목	세부 평가 내용	배점
정량평가 (10점)	경영상태	재무구조 및 경영 상태(신용평가등급)	5
	사업 실적	최근 3년간 유사용역 사업수행실적	5
전략 및 방법론 (25점)	사업 이해도	사업의 특성 및 목표에 대해 업무내용의 이해를 바탕으로 일관성 있는 업무추진이 가능한가를 평가	25
	추진전략	사업 수행 시 일정 및 위험요소를 고려하여 얼마나 타당한 추진 전략을 수립하였는지 평가	
	적용기술	사업에서 적용하고자 하는 기술이 향후 확장성을 고려하였는지, 현실적으로 실현 가능한지 여부를 평가	
기술 및 기능부문 (25점)	시스템 요구사항	요구 규격을 충족하는 장비 제안 여부와 현 시스템과의 인터페이스 및 확장 가능성 여부 평가. 또한 도입 장비의 설치 및 공급 계획, 유지관리에 대한 방안이 구체적으로 기술되어 있는가를 평가	25
	데이터, 성능, 테스트 요구사항	데이터 요구사항 분석을 바탕으로 데이터 전환 계획 및 검증 방법, 데이터 오류 발생 시 처리 방안, 이관 및 운영시 성능에 대한 방안등이 구체적으로 제시되어 있는지 평가	
프로젝트 관리부문 (20점)	사업수행 전문성	참여 업체의 전문성, 유지관리 지원체계 및 방법의 적정성을 평가하며, 업무수행 범위 등이 구체적으로 기술되어 있는가를 평가	20
	보안 요구 사항	보안지침 등을 준수하고 보안정책수립, 보안점검(사전예방 활동), 해킹보고 등 보안문제 발생시 신속한 대응계획 및 자체점검계획이 제시되었는지 평가	
프로젝트 지원부문 (15점)	하자보수 계획	시스템 공급자가 제시하는 하자보수 및 유지보수 계획, 조직, 절차, 범위 및 기간과 이와 관련된 기타의 활동 및 그 제한사항에 대해 평가	15
	시험 운영	시스템 공급자가 개발된 시스템의 시험운영을 위해 필요한 각종 시험운영 방법 등을 구체적으로 제시하였는지 평가	
	교육 훈련	교육계획이 구체적이고 충실하게 제시되었는지를 평가하고, 최신의 정보기술 동향 및 자료의 제공 등 추가적인 기술지원 서비스 제공 방안을 평가	
추가 제안 부문 (5점)		본 사업의 기본 요구사항 외에 사업의 성과 향상, 안정성 확보 및 운영 편의성을 높일 수 있는 추가적인 방안을 제시하였는지 평가	5
계			**100**

나. 정량 평가 기준

1) 경영상태(신용평가등급)

기업신용평가 등급	회사채에 대한 신용평가등급	기업어음에 대한 신용평가등급	평점(점)
회사채에 대한 신용평가등급	A-, A0, A+, BBB-, BBB0, BBB+ 이상	A2-, A20, A2+, A3-, A30, A3+ 이상	5
	BB-, BB0, BB+	B0, B+	4
	B+, B0, B-	B-	3
	CCC+ 이하	C 이하	1

- 신용정보의 이용 및 보호에 관한 법률 제4조(신용정보업 : 신용조회업, 신용평가업)에 의한 신용정보업자가 입찰공고일 이전 가장 최근에 평가한 유효기간(입찰참가서류 제출기한 기준) 내 기업신용평가등급 및 회사채(또는 기업어음)에 대한 신용평가등급(위의 신용정보업자가 신용평가등급, 등급평가일 및 등급유효기간 등을 명시하여 작성한 '신용평가 등급 확인서'를 기준으로 다음의 표에 의하여 평가)
- 평가대상 업체의 기업신용평가 및 회사채(또는 기업어음) 신용평가에 따른 평점이 다른 경우에는 높은 평점으로 평가하며, '신용평가등급확인서'를 제출하지 않은 경우에는 최저등급(CCC+, C))으로 평가

2) 사업 수행실적

(최근 3년간 유사 용역 수행 실적 건수)

구분	5건 이상	4건 이상	3건 이상	2건 이상	1건 이상	0건
점수	5점	4점	3점	2점	1점	0점

- 입찰공고일 기준 최근 3년간 사업수행 실적에 한하며, 도입한 이후 오픈한 시점을 기준으로 함
  - 수행실적증명서
  - 주관사업자로 참여한 실적만 인정

3. 제안평가 유의사항

가. 제안서의 기술적인 측면을 상세히 평가하여 제안요청서에 명시된 요건에 실질적으로 부합하는지 여부를 판단할 것이며, 부합여부 판정을 위해 제안요청서에 명시된 요건에 따라 제안업체가 제출한 자료를 검토함

나. 제안서 내용의 검토와 평가를 위하여 필요한 경우 추가자료 제출 및 설명을 요구할 수 있음. 다만 제안업체가 입증책임을 다하지 아니하여 이행실적의 확인 등이 어려운 경우에는 실적을 인정하지 않음

4. 기타 유의사항

가. 제출서류 관련사항 숙지

1) 본 입찰은 제출된 서류에 한하여 심사 평가하며 세부평가내용은 공개하지 않고, 제출된 서류는 일체 반환하지 않음

2) 제출 서류의 미비 등으로 불이익이 초래될 시에는 이에 대하여 일체의 이의를 제기할 수 없음

나. 비밀유지 의무사항

1) 제안업체는 본 사업과 관련한 제안요청서의 내용이 사업수행을 위한 제안서 제출 이외의 다른 목적으로 사용되어서는 아니 되며, 본 제안요청기관으로부터 배부받은 입찰에 관한 서류 또는 각종 자료 및 입찰과정에서 얻은 정보를 당해 입찰 외의 목적으로 사용할 수 없음

다. 공고내용에 명시되지 않은 사항은 상호 협의 하에 해결하고, 상호 의견차이가 있을 경우에는 제안요청기관의 의견에 따름

라. 계약상의 사업을 수행함에 있어 부실, 조잡 또는 부당하게 하거나, 부정한 행위를 한 업체는 부정당업자 제재 등의 불이익을 받을 수 있음

마. 본 제안요청서에 명시된 모든 조항은 최소한의 사항만을 규정하였으므로 누락된 사항에 대해 문제가 발생되지 않도록 제안업체가 사전 조치를 취하여야 함

【붙임1】

정보화사업 용역업체 정보보호 준수사항

동양미래대학교(이하 본 대학이라 한다.) 정보화사업에 참여하는 용역업체는 다음 사항을 참고하여 정보보호 요구사항을 준수하여야 한다.

1. 일반사항
   가. 본 대학의 정보보호 정책, 지침 및 매뉴얼을 준수하여야 한다.
   나. 본 대학의 자산에 접근하기 위해서는 대학의 접근 통제 절차를 준수하여야 한다.
   다. 본 대학은 계약서의 보안 사항을 준수하고 있는지를 감사할 권한을 가진다.
   라. 본 대학의 감사 시 필요한 근거자료를 제공하고 현장실사에 적극 협조하여야 한다.
   마. 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보호 대책 및 '[별지1]누출금지 대상정보'에 대한 보안관리 계획을 제안서에 기재하여야 한다.
   바. 본 대학의 보안정책을 위반하였을 경우 '[별지2] 사업자 보안 위규 처리기준' 및 '[별지4] 보안위약금 부과 기준'에 따라 위규자 및 관리자를 행정조치하고 민·형사상의 책임을 진다.

2. 제3자의 직원에 대한 보안관리
   가. 참여직원에 대해서 각 개인의 친필 서명이 들어간 보안서약서를 제출한다.
   나. 참여직원은 임의로 교체할 수 없으며, 교체 시 본 대학의 승인을 받는다.

3. 내부 자료에 대한 보안관리
   가. 업무 수행을 위해 제공하는 내부자료는 관리대장을 작성하여 인수·인계 시 직접 서명한다.
   나. 제공된 내부 자료에 대해 복사 및 외부반출을 할 수 없으며, 업무 완료 후 대학에 반환한다.
   다. 제공된 내부 자료는 매일 퇴근 시 반납하여야 한다. 다만, 비밀문서를 제외한 일반 문서는 제3자에 제공된 사무실에 시건장치가 된 보관함이 있을 경우 이를 보관함에 보관할 수 있다.
   라. 본 대학은 제3자에 제공된 사무실에 보관된 자료에 대해서는 수시로 확인할 수 있다.

4. 장비에 대한 보안관리

가. PC(노트북 포함)는 반입시마다 최신 바이러스 백신프로그램 설치와 바이러스 감염 여부를 확인하여야 한다.

나. 업무 수행을 위해 반입된 PC는 업무 종료 시까지 반출 할 수 없다. 다만, 불가피한 경우 본 대학의 승인 후 반출할 수 있다.

다. USB 등의 보조기억매체는 사용할 수 없다. 다만, 불가피한 경우는 본 대학의 승인 후 사용할 수 있다.

라. 업무 종료 시 PC 및 사용된 보조기억매체는 Format하고 본 대학의 승인 후 반출한다.

5. 내·외부망 접근에 대한 보안관리

가. 사용자 계정(ID)은 하나의 그룹으로 등록하고 사용자 계정별로 정보시스템에 접근 권한을 부여토록 한다.

나. 사용자 계정별로 부여된 권한은 불필요 시 곧바로 권한을 해지하거나 계정을 폐기토록 한다.

다. 본 대학은 사용자별로 부여한 계정에 접속하여 저장된 자료와 작업 이력을 확인할 수 있다.

라. 담당자는 서버 관리자로 하여금 내부 서버에 대한 접근기록을 확인하도록 한다.

마. PC(노트북 포함)는 인터넷 연결을 금지한다. 다만, 불가피한 경우는 필요한 보안조치를 실시하고 본 대학의 확인 후 사용한다.

6. 기타 산출물에 대한 보안관리 등

가. 업무 수행 시 생산되는 모든 산출물은 담당 부서의 파일서버에 저장하거나, 본 대학에서 지정한 PC에 저장한다.

나. 업무 수행으로 생산되는 모든 산출물 및 기록은 본 대학이 인가하지 않은 자에게 제공·대여·열람을 금지한다.

다. 업무 수행으로 생산되는 모든 산출물 및 기록의 소유권 및 지적재산권은 본 대학에 있다.

라. 제3자에 의한 보안사고 발생시 민·형사상의 모든 법적 책임은 제3자에게 있다.

마. 보안사고 발생 시 또는 인지 시에는 즉시 본 대학에 통보하여야 한다.

【별지1】

누출금지 대상정보

1. 기관 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성현황 및 정보통신망 구성도
3. 사용자 계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물
5. 용역사업 결과물 및 프로그램 소스코드
6. 국가용 보안시스템 및 정보보호시스템 도입 현황
7. 방화벽 등 정보보호제품 및 라우터·스위치 네트워크 장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」제9조제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9. 「개인정보보호법」제2조제1호의 개인정보
10. 「보안업무규정」제4조의 비밀 및 동 시행규칙 제7조 제3항의 대외비
11. 그 밖에 각급기관의 장이 공개가 불가하다고 판단한 자료

【별지2】

사업자 보안 위규 처리기준

구 분	위 규 사 항	처 리 기 준
심 각	1. 비밀 및 대외비 급 정보 유출 및 유출시도 가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 유출 나. 개인정보·신상정보 목록 유출 다. 비공개 항공사진·공간정보 등 비공개 정보 유출 2. 정보시스템에 대한 불법적 행위 가. 관련 시스템에 대한 해킹 및 해킹시도 나. 시스템 구축 결과물에 대한 외부 유출 다. 시스템 내 인위적인 악성코드 유포	○ 부정당업자 등록 및 계약 해지 ○ 위규자 및 직속 감독자 등 중징계
중 대	1. 비공개 정보 관리 소홀 가. 비공개 정보를 책상 위 등에 방치 나. 비공개 정보를 휴지통·폐지함 등에 유기 또는 이면지 활용 다. 개인정보.신상정보 목록을 책상 위 등에 방치 라. 기타 비공개 정보에 대한 관리소홀 2. 사무실·보호구역 보안관리 허술 가. 통제구역 출입문을 개방한 채 퇴근 등 나. 인가되지 않은 작업자의 내부 시스템 접근 다. 통제구역 내 장비·시설 등 무단 사진촬영 3. 전산정보 보호대책 부실 가. 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 나. 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 다. 개발·하자보수 시 원격작업 사용 라. 저장된 비공개 정보 패스워드 미부여 마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장 바. 외부용 PC를 업무망에 무단 연결 사용 사. 보안관련 프로그램 강제 삭제 아. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)	○ 위규자 및 직속 감독자 등 중징계 ○ 재발방지를 위한 조치계획 제출 ○ 위규자 대상 보안교육 실시

보 통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안·보고 자료를 책상 위 등에 방치 나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용 2. 사무실 보안관리 부실 가. 캐비넷·서류함·책상 등을 개방한 채 퇴근 나. 출입키를 책상 위 등에 방치 3. 보호구역 관리 소홀 가. 통제·제한구역 출입문을 개방한 채 근무 나. 보호구역내 비인가자 출입허용 등 통제 미실시 4. 전산정보 보호대책 부실 가. 휴대용저장매체를 서랍·책상 위 등에 방치한 채 퇴근 나. 네이트온 등 비인가 메신저 무단 사용 다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅·화면보호 패스워드 미부여 또는 "1111" 등 단순 숫자 부여 마. PC 비밀번호를 모니터옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	ㅇ 위규자 및 직속 감독자 등 중징계 ㅇ 재발방지를 위한 조치계획 제출 ㅇ 위규자 대상 보안교육 실시
경 미	1. 업무 관련서류 관리 소홀 가. 진행 중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기·인쇄기 위에 서류 방치 2. 근무자 근무상태 불량 가. 각종 보안장비 운용 미숙 나. 경보·보안장치 작동 불량 3. 전산정보 보호대책 부실 가. PC내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반	ㅇ 위규자 서면·구두 경고 등 문책 ㅇ 위규자 사유서/경위서 징구

【별지3】

사업자 보안관리 준수사항

1. 참여인원에 대한 보안관리

가. 사업자는 정보화사업 개시일부터 종료일까지 보안을 총괄하는 정보보안담당자(정/부)를 지정한다.

나. 인원투입 시 동양미래대학교 정보보안규칙 교육 등 기본 보안교육을 수행하고, 보안 누출 금지조항 및 개인 서명이 포함된 '보안서약서' 및 '기본보안교육 확인서'를 사업 담당 직원에게 제출한다.

다. 인원변동 현황 및 각종 서약서 징구 여부를 '인원관리대장'을 통하여 기록 및 관리한다.

라. 사업 참여인력은 발주와의 승인 없이 사업자 임의로 교체할 수 없으며 교체가 필요할 경우 발주자로부터 사업 참여인력에 대한 증빙서류 등과 함께 사전승인을 받아야 한다.

2. 자료에 대한 보안관리

가. 동양미래대학교로부터 제공받거나 자체 생산한 산출물 중 "별표 1. 누출금지 대상정보"에 해당하는 자료(이하 '누출금지정보"라 한다.)에 대해서는 자료의 인수·인계시 '용역자료인수인계 관리대장'을 작성하여 관리하고(인계자, 인수자가 직접 관리대장에 서명한 후 자료제공), 무단복사 및 외부반출을 금지하며 사업 완료시 관련 자료를 반납·파기한다.

나. 사업과정에서 생산된 모든 산출물은 동양미래대학교에서 제공하는 파일서버나 보안관리자가 지정한 단말기(또는 저장매체)에 저장·관리한다.

다. 사업과정에서 생산된 모든 종이자료(또는 CD) 파기는 파쇄기를 사용한다.

라. 사업 관련 자료는 인터넷 웹하드·P2P 등 인터넷 자료공유사이트 및 개인 메일함에 저장을 금지하고 동양미래대학교와 사업자간 이메일을 이용해 자료전송이 필요한 경우에는 동양미래대학교의 기관메일을 이용, 첨부자료 암호화 후 수·발신해야한다. 단, 누출금지 대상정보는 전자우편으로 수·발신을 금지한다.

마. 상용 이메일의 사용을 금지하며, 동양미래대학교의 기관메일 사용이 필요한 경우 동양미래대학교 정보보안담당자의 승인을 받고 사용해야 한다.

바. 비밀자료는 지정된 사용자만 접근이 가능하도록 하고 다른 정보와 구분하여 보관하여야 하며, 비밀자료를 제외한 일반자료는 사무실 내 잠금장치가 된 보관함에 보관한다.

사. 공유폴더 사용을 금지한다.

3. 사무실·장비에 대한 보안 관리

가. 상주 인력은 배정된 좌석의 정리를 청결히 하고 업무 관련 문서나 이동형 정보통신기기 등 유지관리 용역사업과 관련된 모든 자료는 항상 시건장치가 있는 케비넷에 보관한다.

나. 정보시스템 사용 및 변동 현황을 관리할 수 있는 '전산장비 관리대장'을 구비 및 철저하게 관리한다.

다. 동양미래대학교의 유지관리 및 모니터링용 PC에 설치된 소프트웨어 정보를 기록·관리할 수 있는 '소프트웨어 설치 대장'을 구비 및 철저히 관리하며 사업 담당자 또는 정보보안담당자의 허가 없이 소프트웨어 설치를 금지한다.

라. 동양미래대학교 종합정보지원실 내 사무실 및 장비실 사용 시 출입문이 상시 개방되지

않도록 잠금장치를 관리하고, 외부 사무실 사용 시 CCTV·잠금장치 등 비인가자 출입통제 대책을 마련한다.

마 정보보안담당자 또는 당직근무자 지정을 통해 퇴근 전 문서 및 USB 방치 점검 등 일일 보안 점검을 수행하고, 기록한다.

바. PC등 인가받지 않은 전산기기의 사용 및 무단 반출을 금지한다.

사. 사업 수행 시 단말기의 반입 시 악성코드 감염여부 및 최신 백신업데이트 확인, 보안 점검을 수행해야 하며, 반출시 모든 데이터는 완전삭제 조치한다.

아. 인가받지 않은 USB메모리 등의 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 동양미래대학교의 승인 하에 사용한다.

자. 업무용 및 인터넷용 단말기 내 보안USB 통제 프로그램, 백신프로그램 및 내PC지킴이 등 동양미래대학교 보안 프로그램 설치 및 최신 버전을 유지한다.

차. 사업참여인력 PC에는 USB포트를 물리적인 방법(포트락 등)으로 차단한다.

4. 내·외부망 접근시 보안관리

가. 사업자는 승인받은 장비에 대하여 부여된 권한·목적에 대해 승인받은 기간(최대1년)동안 사용하고, 사용이 종료된 시점에 즉시 반납한다.

나. 사전 승인 없이 동양미래대학교 네트워크에 연결을 금지한다.

5. 보안점검 및 교육

가. 사업자는 보안인식제고를 위해 월1회 자체 보안교육을 하고, 동양미래대학교가 요구하는 보안교육에 참석한다.

나. 사업자측 정보보안담당자는 일1회 자체 보안점검을 실시하고 결과를 사업담당직원에게 제출한다.

※ 상기 사업자 보안관리 준수사항 중 예외적 허용이 필요한 경우에는, 동양미래대학교 정보보안담당에게 예외 허용사항에 대한 보안성 검토를 요청한다.

※ 기타 사항은 동양미래대학교 정보보안업무 세부시행규칙 및 국가 정보보안 기본지침에 따라 용역사업 보안관리를 한다.

【별지4】

보안위약금 부과 기준

1. 위규 수준별로 A~D 등급으로 차등 부과

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	계약해지 및 부정당업자 등록	협의에 의함 (10% 수준)	협의에 의함 (7% 수준)	협의에 의함 (5% 수준)

* 위약금은 〔별지-4〕 위규 내용에 따라 상호 협의로 부과

2. 보안 위약금은 다른 요인에 의해 상쇄, 삭감이 되지 않도록 부과

* 보안사고는 1회의 사고만으로도 그 파급력이 큰 것을 감안하여 타 항목과 별도 부과.

【붙임2】

보 안 확 약 서(대표자용)

본인은 귀 기관과 계약한 오라클 DB 칼럼 암호화 솔루션 도입 사업 용역 사업을 수행함에 있어, 다음 각호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체는 업체 및 사업 참여자가 용역사업수행 중 지득한 모든 자료 및 정보에 대한 유출을 절대 금지하겠습니다.
2. 본 업체는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안서약서 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적책임을 지겠습니다.
3. 본 업체는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

2026년 월 일

서약업체(단체) 대표

소 속 :

직 급 :

성 명 : (서명)

동양미래대학교 정보보안담당관 귀하

【붙임3】

보 안 확 약 서(대표자용)

본인은 귀 기관과 계약한 오라클 DB 칼럼 암호화 솔루션 도입 사업 용역 사업의 수행을 완료함에 있어, 다음 각호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체(단체)는 업체(단체) 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대 금지하겠습니다.
2. 본 업체(단체)는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적책임을 지겠습니다.
3. 본 업체(단체)는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

2026년 월 일

서약업체(단체) 대표

소 속 :

직 급 :

성 명 : (서명)

동양미래대학교 정보보안담당관 귀하

【붙임4】

보안서약서(외부인용)

본인은 _____년_____월____일부로 오라클 DB 칼럼 암호화 솔루션 도입 사업에 있어 다음 사항을 준수할 것을 엄숙히 서약한다.

1. 개인정보보호 및 정보보호 관련 외부인 준수사항을 교육받았고 이를 인지하였으며, 특히 「인적보안관리 지침」의 외부인관련 내용을 준수하겠습니다.
2. 근무 중에 습득한 직무상의 기술 및 기밀에 속하는 사항을 외부에 공개하거나 누설하지 않겠습니다.
3. 동양미래대학교(이하 “본 대학”이라 한다)에서 구매한 응용프로그램 및 대학교에서 개발한 프로그램을 대학교 밖으로 일체 유출하지 않겠습니다.
4. 대학교에서 근무 중 작성한 각종 서류 및 PC에 보관된 일체의 자료를 허가없이 외부로 유출 또는 일시 반출도 하지 않겠습니다.
5. 기타 근무 중 습득한 보안사항이 대학교의 경영에 불이익을 초래할 가능성이 있는 여하한 정보도 외부로 누설하지 않겠습니다.

상기 본인은 본 대학과 체결한 용역을 시행함에 있어 본 대학의 「보안규칙」에서 정하는 바에 따라 상기 사항을 준수할 것이며, 만약 고의 또는 과실로 인한 대학교 재산상의 손해가 발생할 시에는 민·형사상 및 보안상의 책임과 관계법규에 의한 조치를 감수할 것을 서약합니다.

년 월 일

동양미래대학교 총장

서약자	소 속 :	생 년 월 일 :	(인)
	직 위 :	성 명 :	(인)
서약집행자[1]	소 속 :	생 년 월 일 :	(인)
	직 위 :	성 명 :	(인)

1) 대학에서 작성함

【붙임5】

원격접속 보안서약서

성 명	
생년월일	
소 속	

본인은 동양미래대학교(이하 “대학”이라 한다)에 년 월 일부로 원격접속을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 대학의 제한구역 및 통제구역에 무단으로 출입하지 않는다.
2. 대학의 자산을 불법으로 유출, 변조하거나 훼손하지 않는다.
3. 대학의 자산을 개인적인 목적이나 이익을 위하여 사용하지 않으며, 허가된 용도로만 사용한다.
4. 허용되지 않은 정보자산에 접근을 시도하거나 정보보안 기능을 우회하는 시도를 하지 않는다.
5. 업무상 취득한 대학 또는 제3자 소유의 정보를 대학의 승인 없이 누설하지 않는다.
6. 대학의 통신망을 이용하여 외부인 접근이 금지된 타 대학이나 기관의 통신망 또는 시스템에 임의로 접속을 시도하지 않는다.
7. 대학의 자산(정보 포함)을 사용 후에는 즉시 대학에 전부 반환한다.
8. 기타 대학의 정보보안 관련 규정을 준수한다.

본인은 위의 사항을 숙지하여 이를 성실히 준수할 것이며 만일 이를 위반하였을 경우 민·형사상의 책임을 감수함은 물론 대학에 끼친 손해에 대해 지체 없이 변상·복구할 것을 서약합니다.

년 월 일	
서약자	(인)

동양미래대학교 정보보안담당관 귀하