경남대학교 홈페이지 운영 및 관리 지침

제정 2021. 9. 15.
소관부서 정보전산원 정보전산팀

제1조(목적) 경남대학교 내에서 운영되는 대학, 행정부서, 단과대학, 학과(부), 연구소 기타 학내 기구의 홈페이지 구축 및 운영지원을 위한 제반사항을 규정하고 이용자들에게 보다 유용한 콘텐츠를 제공하기 위한 규정을 정함에 있다.

제2조(적용범위) 이 지침의 적용범위는 경남대학교 내 구축되어 공식 도메인을 사용하는 대학홈페이지 및 하위홈페이지 그리고 기관홈페이지로 한다.

제3조(용어의 정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. 홈페이지라 함은 특정 서비스를 위해 구성된 웹페이지의 집합체로 웹사이트라고도 지칭된다.
2. 공식도메인이라 함은 경남대학교에서 정식으로 사용하는 도메인으로서 kyungnam.ac.kr, uok.ac.kr이 있으며, 지침에 표기된 www.kyungnam.ac.kr의 경우는 www.uok.ac.kr도 포함한다.
3. 대학홈페이지라 함은 정보전산원에서 직접 관리하는 대학의 메인 홈페이지(www.kyungnam.ac.kr)를 지칭한다.
4. 대학홈페이지의 하위 홈페이지는 행정부서, 단과대학, 학부(과), 연구소 등의 학내 기구를 위해 대학홈페이지 하위에 개설되는 웹페이지(www.kyungnam.ac.kr/~~)를 지칭한다.
5. 기관홈페이지라 함은 행정부서, 단과대학, 학부(과), 연구소 등의 학내 기구를 위해 대학홈페이지와 별도로 구축되는 웹페이지(~~.kyungnam.ac.kr)를 지칭한다.
6. CMS라 함은 Content Management System의 약자로 홈페이지 구축 및 운영을 지원하는 솔루션이 다.
7. 콘텐츠라 함은 홈페이지에 삽입되는 텍스트, 이미지, 사운드, 비디오 등의 재료를 말한다.
8. 고유식별정보라 함은 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호에 해당하는 정보를 말한다.

제4조(담당자 임명) 조직별로 홈페이지(대학홈페이지, 하위홈페이지, 기관홈페이지)의 전반을 관리하고 콘텐츠를 유지보수하는 등의 업무를 수행할 홈페이지 담당자를 각 조직의 부서장이 지정한다.

제5조(담당자 역할) ① 담당 홈페이지(대학홈페이지, 하위홈페이지, 기관홈페이지)의 운영 및 관리는 각 담당자가 총괄한다.

② 하위홈페이지 담당자는 CMS 시스템을 사용하여 홈페이지를 직접 관리하는 것을 원칙으로 한다.

③ 기관홈페이지 담당자는 홈페이지 운영 및 관리주체를 선정한다(필요시 예산을 확보한다).
④ 각 홈페이지(대학홈페이지, 하위홈페이지, 기관홈페이지) 담당자는 보안 취약사항 관련 공지사항을 숙지하고 적절한 조치를 취한다.
⑤ 홈페이지(대학홈페이지, 하위홈페이지, 기관홈페이지) 담당자는 다음의 콘텐츠 관리를 수행한다.

1. 이용자들에게 잘못된 정보전달을 방지하기 위하여 변경되었거나 더 이상 유효하지 않은 과거 자료는 삭제하고 항상 최신의 게시물과 텍스트, 이미지 등의 콘텐츠들로 유지한다.
2. 링크오류 수정, 타 웹사이트를 링크할 경우, 해당 웹사이트의 정보에 대한 지식재산권과 보안책임을 명확히 하여야 하고 필요시 주의사항을 표시한다.
3. 아래의 각목에 유의하여 게시물을 관리한다.
   가. 개인정보(주민등록번호, 운전면허번호, 여권번호, 외국인등록번호, 휴대전화번호 등)를 게시물로 등록하지 않는다.
   나. 각 언론기관의 뉴스 등 타인의 저작물을 저작권자의 동의 없이 무단으로 사용하지 않는다. 저작권 침해는 저작권법에 의거 처벌 대상이 되며 별도로 민사상 손해 배상 책임을 질 수 있다.
   다. 웹사이트에 게재되는 모든 정보에 대하여 매일 점검하고, 타인의 명예를 손상시킬 수 있거나 사생활침해 등 불법정보에 대하여는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 준용하여 처리한다.
   라. 허위사실유포, 욕설, 비방, 광고성 글, 뉴스무단복제(기타 저작권 관련 게시물) 등은 게재하지 않는다. 고의적인 악용이나 도배성 글 게재 시에는 ID 또는 IP 차단 등으로 서비스 이용에 제약을 받을 수 있다.
   마. 고유식별정보가 홈페이지 게시판 등에서 유출되지 않도록 모니터링한다.
   바. 홈페이지에 삽입되는 이미지나 글의 글꼴, 게시물, 동영상 등이 저작권에 위배되지 않도록 사전에 확인한다.
   사. 관리자 페이지 주소와 아이디, 패스워드를 타인에게 노출 및 제공하지 않는다.

제6조(정보전산팀 역할) 대학 메인 홈페이지 관리부서인 정보전산팀은 다음과 같은 업무를 수행한다.

1. CMS 솔루션을 운영하고 관리한다.
2. 대학홈페이지 내 메인페이지를 관리한다.
3. 각 조직의 담당자가 요청하는 내용을 접수받아 가능한 범위내에서 지원한다.
   단, 템플릿 변경・추가와 같은 솔루션 수정사항은 제외하며, 각 조직의 홈페이지 신규 제작・구축에 가늠되는 사항은 협의를 통해 지원범위를 결정한다.
4. 연1회 이상 각 조직의 홈페이지 담당자를 대상으로 CMS 활용 교육을 실시하고, CMS 활용에 대한 문의사항에 응대한다.
5. 대학 내 홈페이지(대학홈페이지, 하위홈페이지, 기관홈페이지) 현황을 관리하고 담당자가 홈페이지를 적절히 운영할 수 있도록 지도한다.

제7조(홈페이지 신규 구축) 홈페이지 신규 구축은 다음의 내용을 준수하여 제작한다.

1. 대학홈페이지 및 하위홈페이지 자체 제작의 경우
   가. 홈페이지 첫화면 구성(안), 홈페이지 메뉴(안), 메뉴별 페이지에 사용할 이미지, 동영상,

텍스트 등 콘텐츠를 준비한다.

나. 홈페이지 첫화면 구성(안), 준비된 콘텐츠와 별첨1의 신청서를 작성하여 정보전산팀 담당자와 협의한다.

다. 조직별로 지정된 템플릿으로 제작한다.

2. 기관홈페이지 외부용역 제작의 경우

가. 별첨2의 홈페이지구축 및 운영 가이드를 참조하여 구축한다.

나. kyungnam.ac.kr의 하위 도메인을 사용하거나 학내 IP로 서비스할 경우 정보전산원에 외부와 연결을 요청한다.

부칙

이 규정은 2021년 9월 15일부터 시행한다.

[별첨1]

경남대학교 CMS 홈페이지(대학홈페이지 내 하위홈페이지) 구축 신청서

담당자	소속		전화번호	
	성명/직급		이메일	
학과(부)장	홍 길 동 (인)		홈페이지ID (알파벳소문자 사용)	홈페이지 하위주소와 관리자 계정으로 이용 ex) eng
메뉴구조				
1-depth(대메뉴)		2-depth(하위메뉴)	3-depth(하위메뉴)	페이지 유형
학부소개		학부소개		일반페이지
		교육목표		일반페이지
		교육과정		일반페이지
취업/진로		진출분야		일반페이지
		자격증정보		일반페이지
		취업소식		일반페이지
		취업게시판		일반게시판
예비대학생		입학안내		일반페이지
		장학제도		일반페이지
		기숙사안내		일반페이지
대학원		전공소개		일반페이지
		교육과정		일반페이지
		대학원게시판		일반게시판
커뮤니티		알림게시판		일반게시판
		학과수업자료실		일반게시판
		자유게시판		일반게시판
		Q&A		Q&A게시판
		FAQ		FAQ게시판

[별첨2]

기관홈페이지 구축 및 운영 가이드(외부용역개발)

① 구축 관련 주요활동

1. 홈페이지 구축에 필요한 예산확보
   ※ 개발용역비, 소프트웨어 구입비, 장비구입비, 호스팅비 등을 고려
2. kyungnam.ac.kr 도메인을 사용할 경우 정보전산팀에 도메인 신청서 제출
   ※ 공유파일(X드라이버) > 양식_메뉴얼 > 양식 > 도메인등록 및 방화벽 오픈 신청서.hwp
3. 구축범위, 기간, 주요 서비스 및 콘텐츠를 정리한 계획서 작성
4. 구축 의뢰를 위한 제안요청서 작성 및 검토(입찰 시 필수)
5. 수의계약 혹은 입찰
   ※ 입찰인지 수의계약 건인지 여부는 구축 총금액에 따라 결정되며 자체처리인지 구매의뢰 건인지 여부는 예산 계정과목의 성격에 따라 결정됨
   ※ 입찰 건의 경우 제안요청서 작성 후 보안성 검토실시
6. 계약체결

② 구축시 준수사항

구분	주요 내용
웹 호환성	(개요) 웹표준 기술을 사용, 다양한 웹브라우저 등 이용환경에 관계없이 동등한 서비스 제공 (고려사항) - 웹표준 문법((X)HTML, CSS)을 준수하고 웹호환성(동작, 레이아웃)을 확보하도록 개발 - 기획 단계부터 비표준기술 적용을 배제하여야 함 - 개발 시 점검 툴 등을 활용하여 호환성 여부를 점검 - 웹사이트의 구축・개선・유지보수 및 운영 시, 비표준기술 제거를 위해 노력해야 함 ・ HTML5를 적용한 웹사이트 구축을 통해 되도록 웹표준 및 호환성을 확보 (참고) 전자정부 웹사이트 품질관리 지침(행정안전부) 웹접근성 및 웹호환성 수준진단 점검지표 2019(행정안전부)
웹 접근성	(개요) 이용자가 신체적 또는 인지적 제약 등으로 인한 불편함 없이 웹사이트에서 제공하는 정보와 위치식별 등 기능에 쉽게 접근할 수 있도록 보장 (고려사항) - 웹콘텐츠에 대해 인식, 운용, 이해가 용이하도록 구현하고, 표준을 준수함으로써 어떠한 기술로도 접근이 가능토록 구현 - 개발 시 점검 툴 등을 활용하여 접근성 여부를 점검 (참고) 한국형 웹 콘텐츠 접근성 지침 2.1(과학기술정보통신부 국립전파연구원)
웹 개방성	(개요) 이용자가 아무런 제약 없이 웹에 공개된 정보에 접근하여 이용할 수 있도록 제공 (고려사항) - 웹사이트가 특정 검색엔진이나 검색로봇의 접근을 차단하지 않도록 해야 하며, 페이지 정보 수집을 거부하거나 페이지별 URL을 차단하지 않도록 해야 함 - 개발 시 웹사이트 자가진단지표, 점검 툴 등을 활용하여 웹 개방성 여부를 점검 (참고) 구글/네이버 ‘검색엔진 최적화 기본가이드’ 웹접근성 및 웹호환성 수준진단 점검지표 2019(행정안전부)
웹 최적화	(개요) 사용자의 요청에 의해 웹사이트가 브라우저에 표시되는 데까지의 응답시간과 웹사

구분	주요 내용
(접속성)	이트에 제공된 링크의 연결을 최적의 상태로 제공 (고려사항) - 웹페이지 용량(3MB) 이하, 요청횟수 최소화, 응답속도 3초 이하 등 웹 최적화를 구현하여 이용자 편의성 확보 - 웹사이트 자가진단지표 및 점검 툴 등을 활용하여 웹 최적화 여부를 점검 (참고) 전자정부 웹사이트 UI·UX 가이드라인 부록5(행정안전부)
사용자 중심의 UI·UX (편의성)	(개요) 웹사이트의 디자인, 스타일, 기능 등을 이용자 중심으로 구현하여 편의성 확보 (고려사항) - 해당 웹사이트에 대한 사용자의 요구사항과 문제를 정의하고, 사용자에게 필요한 정보 및 서비스를 효율적이고 일관성 있게 제공하도록 노력해야 함 - UI·UX 설계, 구현, 테스트 단계에서 전자정부 웹사이트 UI·UX 가이드라인을 활용하여, 사용자경험 적용을 위한 사항들이 잘 준수되었는지 점검 (참고) 전자정부 웹 사이트 UI·UX 가이드라인(행정안전부)
개인정보 보호	(개요) 웹사이트에서 수집, 처리하게 될 개인정보를 정의하고 이에 대한 영향도를 사전 분석하고 이를 고려하여 개발함으로써 운영 과정에서 발생할 개인정보 유출·노출을 예방 (고려사항) - 필요 시 개인정보 영향평가를 통하여 개인정보 침해가 우려되는 위험요인을 분석하고 이에 대한 개선방안을 고려하여 구축 - 개인정보보호법 등 관계법령에서 요구하는 개인정보 처리 제한 사항 및 기술적 보호조치에 대해서 이행에 필요한 사항을 식별하고 이에 따라 구축이 될 수 있도록 함 (참고) 개인정보보호법(개인정보보호위원회) 개인정보의 안전성 확보조치 기준(개인정보보호위원회) 표준 개인정보 보호지침(개인정보보호위원회) 개인정보 영향평가에 관한 고시(개인정보보호위원회)
개발보안	(개요) 웹사이트 개발 시 해킹 등 사이버공격을 유발할 가능성이 있는 잠재적인 보안약점이 없도록 개발 (고려사항) - 투입인력은 개발 투입 전에 소프트웨어 개발보안 교육 실시 - 웹사이트에서 발생 가능한 유형별 보안약점을 식별하고 이를 예방하기 위하여 개발가이드라인을 참조하여 개발 - 행정기관 및 공공기관 정보시스템 구축·운영 지침 [별표3](소프트웨어 보안약점 기준)의 보안약점이 없도록 소프트웨어 개발·변경 추진 * 행정기관 및 공공기관 정보시스템 구축·운영 지침 제50조(소프트웨어 개발보안 원칙)~제52조(보안약점 진단기준) ※ 제안서 평가 시 소프트웨어 보안약점 진단도구 사용여부, 개발절차와 방법의 적절성, 소프트웨어 개발보안 관련 교육계획의 적정성 등 반영 고려 - 개발 후 유형별 보안약점에 대한 진단, 발견된 보안약점에 대해 조치 후 서비스 오픈 - 보안약점에 대해서는 운영·관리 단계에서 주기적, 비주기적(서비스 환경 변화요인 발생 등)으로 지속적인 진단 및 조치활동 이행 (참고) 소프트웨어 개발보안 가이드 2019(행정안전부) 시큐어코딩 가이드 2019(행정안전부) 소프트웨어 보안약점 진단가이드 2019(행정안전부) 공개SW를 활용한 소프트웨어 개발보안 점검가이드 2019(행정안전부)

구분	주요 내용
표준 프레임 워크	(개요) 시스템 개발·운영 시 필요한 기능(공통 컴포넌트) 및 환경(실행, 개발, 운영, 관리 환경 등)들을 표준화하여 미리 구현해 둔 것 (고려사항) - 웹사이트 구현에 요구되는 기능들을 정의하고, 해당 기능이 표준프레임워크를 통해 활용 가능할 경우 적극 활용
솔루션 도입	(개요) 시스템 개발·운영 시 적용되는 응용 소프트웨어 등 솔루션 도입 시 고려사항 (고려사항) - 웹사이트의 세부적 요구기능을 사전 정의한 후 솔루션 도입여부를 판단함 - 솔루션의 기능표 및 비교 기능표, 장비 요구사항, 솔루션 라이선스 방식과 가격, 커스터마이징 범위와 기술지원 범위, 솔루션 납품 기획서(포트폴리오), 하자보수 및 유지보수 지원 등을 기본적으로 확인하여야 함 - 솔루션에 의해 콘텐츠를 만들거나 웹사이트의 UI·UX에 영향을 미치는 경우 웹 표준, 정보 접근성(소프트웨어 접근성)을 준수하고 있는지 확인하여야 함
로그인 · 사용자 인증	(개요) 이용자 식별을 위한 로그인 혹은 사용자 인증 방식에 대한 고려사항 (고려사항) - 웹사이트 서비스 유형에 따라 이용자 식별이 필요한지 검토가 필요하며, 이용자 식별이 필요한 경우에도 본인확인이 필요한 수준인지 판단 필요 * 본인확인 수단 예시 : ▲(전자서명법) 공동인증서(구.공인인증서), 다양한 전자서명인증서비스, ▲(정보통신망법) 아이핀, 휴대폰을 통한 본인확인, ▲(전자정부법) 신용카드 등록정보를 통한 신원확인 등 - 이용자 식별이 필요한 경우 웹사이트의 취급정보, 중요도 및 영향도 등을 자체 점검하고, 그 결과에 따라 적정한 인증수단을 선정해야 함 * 행정안전부(www.mois.go.kr)> 정책자료> 참고자료> “공공웹사이트 인증수단 소개서” 활용 - 특히, 대민서비스의 이용자를 확인(식별)하는 경우 여러 전자정부 웹사이트를 하나의 아이디로 편리하게 이용할 수 있도록 행정안전부가 제공하는 통합로그인(통합인증) 공통기반인 ‘디지털원패스’를 활용하도록 검토해야 함 * 「행정기관 및 공공기관 정보시스템 구축·운영 지침」 제14조의3(사용자 확인)

③ 주요산출물

산출물명	산출물 설명
메뉴구성도	메인메뉴, 서브메뉴, 유틸리티 메뉴 등 전체 구성정보를 하나의 구조도로 정리한 문서
데이터명세서	콘텐츠 분류와 서비스 구성에 대한 자료 및 네이밍 규칙정의
ERD(Entity Relation Diagram)	데이터베이스(DB)의 구성 및 관계를 알 수 있는 자료로 각 테이블의 물리적 논리적 관계를 설명해주는 다이어그램으로 테이블명세서를 포함
테스트시나리오 및 결과서	서비스 테스트를 위한 자료로 테스트할 항목을 순차적 방식으로 구분하여 정의하고 이에 따른 테스트 결과를 체크하는 문서로 개발결과물에 대한 완성도를 확인하는데 활용
프로그램 개발명세서	개발된 프로그램에 대한 명세서로 운영 중 프로그램의 개선이 필요시 활용되는 자료
프로그램 목록	개발 프로그램에 대한 기능 및 파일명 위치 등을 표시한 목록자료
운영자매뉴얼	서비스 운영자가 운영을 위해 알아야 하는 시스템, 서비스 관리 등에 대한 매뉴얼
사용자매뉴얼	일반 사용자가 서비스 사용을 위해 알아야 하는 가이드 문서로 홈페이지의 메뉴별 이용방법에 대해 기술

④ 운영관리

기관홈페이지를 구축한 부서는 홈페이지의 콘텐츠관리, 정보 및 시스템 보안을 위해 자체 홈페이지 운영 및 관리 체계를 구축해야 한다.

1. 콘텐츠관리
   가. 웹사이트 등의 모든 콘텐츠에 대한 정보오류, 링크오류, 자료현행화 등을 수시로 점검하고 관리 강화
   나. 자료 작성 및 현행화할 경우, 지식재산권에 저촉되지 않도록 주의
   다. 웹사이트에 게재되는 모든 정보에 대하여 매일 점검하여 타인의 명예를 손상시킬 수 있거나, 사생활 침해 등 불법정보에 대하여는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 준용하여 처리
   라. 타 웹사이트를 링크할 경우, 해당 웹사이트의 정보에 대한 지식재산권과 보안책임을 명확히 하여야 하고 필요시 주의사항 표시
   마. 비공개 자료 및 개인정보가 유·노출, 위·변조 보안 조치 및 훼손 여부 확인

2. 정보 및 시스템 보안
   가. 운영체제 등 웹 서버에 탑재되어 운영 중인 각종 SW에 대한 패치 실시, 불필요한 서

비스나 SW 등은 동작을 중지시키거나 제거하여 안정적인 운영

※ OS, SW 등의 패치로 인한 장애를 예방하기 위해 패치 절차 등을 규정하여야 함

나. 사용자계정 관리

1) 시스템관리자 등 사용자계정(ID) 관리자는 사용자계정의 비인가자 도용 및 정보시스템 불법접속 등을 방지하기 위해 노력

가) 신규 사용자계정 생성 시 신청서 작성, 신원확인 등의 절차를 거쳐 발급

나) 시스템관리자 등 사용자계정 관리자는 정보시스템별로 계정발급현황을 작성·관리

2) 사용목적 및 권한에 따라 관리자와 사용자계정으로 분류・관리

가) 모든 계정은 지정된 자만이 사용하고 부여된 계정을 공동으로 사용 금지

나) 비밀번호 등 사용자 식별·인증 수단이 없는 사용자계정은 사용 금지

3) 외부 사용자 계정부여는 불허하되, 부득이한 경우, 정보보안담당관의 책임하에 유효기간을 설정하는 등 보안조치를 강구한 후 허용

4) 계정을 주기적(사용자 6개월, 관리자 3개월)으로 점검하여 접근 권한을 재검토하고 장시간 사용하지 않는 계정은 휴면계정으로 관리 및 신속히 삭제

다. 웹 보안 취약점 점검 및 대응

1) 행정기관 등이 제공하는 웹서비스의 안정성 및 신뢰성을 확보하기 위하여 웹사이트의 웹 보안 취약점에 대한 상시대응 체계 마련

2) 웹 프로그램의 취약점 점검 및 업데이트 절차(작업신청, 검토, 승인, 작업, 결과보고 등)를 수립하여 취약하거나 승인되지 않은 프로그램이 서비스되지 않도록 관리

⑤ 폐기

1. 홈페이지 운영 엔진(IIS, Apache, Tomcat 등)을 중단 또는 삭제
2. 홈페이지 소스 삭제, 개인정보가 포함된 문서 삭제
3. DB파일 삭제
4. 정보전산팀에 도메인 삭제 신청서 제출

※ 공유폴더(X드라이버) > 양식_메뉴얼 > 양식 > 도메인삭제신청.hwp

참고) 행정기관 웹사이트 구축운영 가이드(2021년 3월)

정보전산팀 회보 제286호 홈페이지 및 업무용 서버 등 운영 관련 안내(2019년 9월)