보안,경비,비상상황 대응 규칙

ECO융합섬유연구원
Korea Institute of Convergence Textile

보안, 경비, 비상상황대응 규칙

2010. 08. 01 제정, 2013. 11. 28 개정
(통폐합 : 보안업무지침, 비상상황 대응규칙, 경비근무규칙)
2014. 05. 21 개정, 2015. 11. 10 개정
2016. 07. 10 개정, 2018. 05. 14 개정
2021. 06. 30 개정, 2024. 01. 09 개정

제1장 총 칙

제1조(목적) 이 규칙은 ECO융합섬유연구원「위원회운영 및 재산의 사용·관리 규정」을 보완적 규칙으로 정함을 목적으로 한다.<개정 18.05.14>

제2조(적용범위) 본 규칙은 ECO융합섬유연구원(이하"연구원"이라 한다) 본관동, 공장동 및 부속시설 등 기타 보안업무상 조정 또는 관리해야 할 사항에 대하여 적용한다.

제3조(보안담당자 및 그 책무) ①「인사규정」에 의거 채용된 직원은 아래 직무와 관련하여 보완업무담당자가 된다.

1. 연구원 재산관리규정 제4조에 의한 재산총괄자, 시설관리자
2. CCTV, 전기, 전산실, 통신실 등(이하 "정보통신분야"라 한다)에 대한 정보통신분야 담당자
3. CCTV, 전기, 전산실, 통신실 등(이하 "정보통신분야"라 한다)에 대한 담당자
4 . 보안담당자는 다음 각 호의 업무를 수행한다.

가. 본관동, 공장동 및 연구원 부대시설에 대한 보안사항 유지관리 (교체, 정비, 수선 등)
나. 대 내·외 보안진단 및 보안업무 대응에 관한 사항
다. 기타 보안업무 전반에 관한 체계적 유지관리 및 교육에 관한 사항

제4조(보안교육) 각 분야별 보안업무담당자는 재산총괄자에게 서면보고 후 직원을 대상으로 하여 연1회 이상 정기 보안교육을 실시하여야 한다.

제5조(사이버·보안 진단의 날 시행) ① 각 보안담당자는 년 1일을 '사이버·보안·방화·방범진단의 날'로 지정하여 다음 각 호의 사항을 시행한다.

1. PC 진단프로그램 이용한 개인 PC 진단 및 취약점 제거, 보완
2. 비밀전수조사, 비밀안전지출 및 파기계획 점검
3. 기타 자체 시행계획에 반영된 사항 및 재산총괄자의 지시사항

② 각 보안담당관은 사이버·보안·방화·방범 진단 결과 발견된 문제점을 즉시 선 시정조치 후 보고(서면 또는 구두)하여야 한다.

제2장 보안관리

제6조(보안사고) 보안사고라 함은 다음 각호와 같다.

1. 비밀의 누설 또는 분실
2. 연구원 중요시설 및 장비의 화재·파괴사고
3. 연구원 전역에 대한 불법 침입사고
4. 기타 보안사고

제7조(보안사고의 보고) ① 보안 사고를 발견한 직원 또는 이를 인지한 직원은 재산총괄책임자, 관계실무자 또는 보안담당자에게 즉시 보고하여야 한다.

② 보안담당자는 제1항과 관련하여 지체 없이 다음 내용으로 원장, 이사장에게 보고하고 민형사상의 문제 사안에 대해서는 가장 가까운 경찰관서에 신고하고 전말조사결과 조치에 따른다.

1. 일시, 장소
2. 사고의 대인, 대물사항
3. 사고내용(육하원칙에 의거)
4. 조치사항

③ 보고를 받은 재산 총괄자는 이사장의 의견을 받아 지도감독 기관 및 관련 유관기관에 통보하여야 한다.

④ 보안사고의 내용은 발생경위 및 이에 대한 전말조사가 종결될 때까지 공개하여서는 아니 된다.

제8조(보안사고의 보고불이행에 대한 조치) 보안사고가 발생하였을 때에 사고를 범하였거나 이를 인지하였음에도 불구하고 소정의 보고조치를 이행하지 않았거나 사고를 은닉한 자는 물론 관계된 직원에게는 관계법규에 의하여 조치하여야 한다.

제9조(보안사고의 조사 처리) ① 다음 각 호에 해당되는 자에 대하여 그 전말을 조사, 연구원 관계규정에 의거 처분 또는 사법기관 등의 관계기관에게 조치를 요구할 수 있다.

1. 연구원에서 보안을 요구하는 문서 또는 각종자료를 분실 또는 누설한자
2. 연구원에서 보안을 요구하는 문서 또는 각종자료를 일반문서로 취급 처리한 자
3. 연구원에서 보안을 요구하는 문서 또는 각종자료를 보관용기를 잠그지 않고 퇴근한 자
4. 제3조의 책무외의 자에게 위임하여 보관 업무를 취급하게 한 자
5. 연구원에서 보안을 요구하는 문서 또는 각종자료를 방조, 방임, 위법, 탈법 등으로 연구원의 제반규정에 반하는 행위자
6. 연구원 제반업무를 규정대로 이행치 않아 보안업무에 중대한 지장을 초래케 한 자
7. 기타 제1호 내지 제6호 이외에 연구원에 피해를 준 위반한 자

제3장 정보 통신

제10조(기본방향) 보안담당자는 정보통신 수단에 의한 각종 연구원정보의 누설을 방지하고 보호하여야 하며 다음과 같은 정보통신보안 기본활동을 수행하여야 한다.

1. 정보통신보안 계획수립 및 시행
2. 정보통신보안 교육계획 수립 시행
3. 정보통신시스템의 취약성 진단·분석 및 보안대책 수립 시행
4. 정보통신보안 위규적발 강화 및 사고조사 처리
5. 악성코드·해킹 등 사이버테러 위해요소 제거
6. 기타 정보통신보안 제반 사항

제11조(PC 등 보안관리) ① 보안담당자는 PC, 단말기(업무용), 노트북 등(이하 "개인용 장비"라 한다)을 사용할 경우에 취급자 또는 관리책임자(이하 "관리책임자"라 한다)를 지정하여야 한다.

② 관리책임자는 비인가자가 무단으로 개인용 장비 등을 조작하여 전산자료를 유출하거나 위·변조 및 훼손시키지 못하도록 다음 각 호에 정한 보안대책을 강구하여야 한다.

1. 장비별·자료별 및 사용자별로 비밀번호 사용
2. PC 하드웨어 (CMOS 등), 운영체제 로그인 및 화면보호기에 각각 비밀번호 설정
3. 10분 이상 작업을 중단할 경우 비밀번호가 적용된 화면보호기 설정
4. 백신, PC용 침입차단시스템 등 운용 및 주기적(최소 월1회이상) 보안패치 실시
5. P2P, 해킹용 S/W 등 업무와 무관하거나 보안에 취약한 프로그램의 사용금지

③ 관리책임자는 개인용 장비 등을 교체·반납 또는 폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크에 수록된 자료가 유출 또는 훼손되지 않도록 보안조치를 강구하여야 한다.

④ 개인용 장비를 반출·입할 경우 별표1. 보조기억매체(전산장비 포함) 반출·입대장에 등재한 후 관리책임자의 승인을 얻어 보안조치를 한 후 반입 또는 반출할 수 있다.

⑤ 관리책임자는 출장 또는 휴가 등으로 장시간 이석할 때에 휴대용 단말기를 시건장치가 있는 사물함 등 안전한 장소에 보관하거나 도난방지 케이블을 설치하여 관리하여야 한다.

⑥ 기타 연구원의 정관, 제반규정을 준용해야 한다

제12조(정보통신시스템 보안관리) ① 보안담당자는 정보통신시스템(정보통신망 포함)의 효율적인 보안관리를 위하여 관리책임자(이하 "시스템관리자"라 한다)를 지정 운용할 수 있다.

② 시스템관리자는 운영되는 정보통신시스템이 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 하며, 보안취약점을 제공할 수 있는 다음 각 호의 프로그램의 설치를 제한하여야 한다.

1. P2P, 웹하드 등 파일 공유 프로그램

2. 메신저 프로그램 등

③ 시스템관리자는 서버를 도입할 경우 별표2의 정보통신시스템 관리대장에 따라 그 하드웨어 목록을 유지·관리해야 하며, 비인가자가 접근할 수 없도록 물리적인 접근통제 장치가 마련된 공간에 서버를 설치해야 한다.

④ 시스템관리자는 소관 시스템의 안정적 운영을 위해 다음 각 호에 따라 관리해야 한다.

1. 신규로 설치되는 시스템은 취약점 점검 및 제거 후 네트워크에 연결
2. 사용 중인 운영체제는 최신의 패치 프로그램 설치, 주기적인 패치 실행
3. 설치·운영 중인 서버의 수시 보안취약점 발굴 및 보안조치

⑤ 시스템관리자는 외부자가 전산실에 출입하여 서버와 관련된 작업을 할 경우 이를 운영하는 담당직원 입회・감독하도록 해야 한다.

⑥ 비인가자가 정보통신시스템에 침입한 사실을 인지한 경우에는 시스템 보호를 위한 접속차단 등 조치를 취하고 보안담당관에게 통보 및 보안대책을 강구하여야 한다.

제13조(인터넷 등 상용망 연동) ① 연구원은 관련 기관, 단체 등과 외부 정보통신망을 연결하고자 하는 경우에 보안관리 책임한계 설정, 정보통신의 제공범위 및 이용자 접근제한 등에 대해 통신망 보안대책을 수립·시행하여야 한다. 이 경우 다음과 같은 보안조치를 하여야 한다.

1. 접속 자료의 주기적 분석
2. 보안도구를 이용한 네트워크 취약성 수시 점검
3. 보안적합성이 검증된 침입차단·탐지 시스템 설치 운용 등 보안대책 실시
4. 연결지점을 지정 운영하여 임의 접속 차단

② 연구원은 정보통신망을 상용망(인터넷 포함)이나 다른 기관, 단체와 정보통신망을 연계하기 위한 보안관리 연결지점을 운용할 경우에는 비인가자의 무단침입(불법접속)이나 악성코드 및 사이버공격을 방지하기 위하여 연구원이 검증한 보안시스템의 설치·운용 등 보안대책을 강구하여야 한다.

③ 연구원은 정보통신망 및 각종시스템에 사용되는 “IP주소”를 별표3의 IP주소 관리대장에 등재 대외비 이상으로 체계적 관리하여야 한다.

④ 연구원은 인터넷을 통한 불법 사이트 접속이나 프로그램 다운로드를 금지하여야 하며, 개인용 장비에서 음란·도박·증권 등 업무와 무관한 인터넷 사이트 접근에 대한 통제대책을 강구하여야 한다.

⑤ 연구원은 비밀을 취급하는 정보통신망 또는 주요정보통신기반시설의 네트워크는 상용망과 분리·운용하여야 한다.

제14조(홈페이지 등 웹서버 보안관리) ① 연구원은 외부자에게 공개할 목적으로 설치되는 웹서버 등 각종 공개서버는 내부망(업무망)과 분리하여 운영하고 보안적합성이 검증된 침입차단·탐지시스템을 설치하는 등 보안대책을 강구하여야 한다.

② 보안담당자 또는 시스템관리자는 공개서버의 서비스에 필요한 프로그램을 설치하고 시험하기 위해 사용된 도구(컴파일러 등)는 완료 후 사용이 제한되도록 보안기능을 설정하거나 삭제하여야 한다.

③ 시스템관리자는 보안사고에 대비하여 서버 설정 정보, 저장 자료 및 프로그램(Source Code)에 대하여 정기적인 백업체계를 구축하여야 한다.

④ 시스템관리자는 홈페이지 게재내용에 비밀 등 비공개 자료가 포함되지 않도록 하여야 하며, 공개서버를 통해 개인정보가 유출 또는 위·변조되지 않도록 보안대책을 강구하여야 한다.

제15조(전자우편 등 보안관리) ① 연구원의 상용메일의 접속을 차단하고 직원들이 업무용으로 허용된 e-mail만 사용토록 해야 한다. 다만, 인터넷망과 업무망이 분리된 경우에 인터넷망에서 상용e-mail의 접속을 허용할 수 있다.

② 연구원은 e-mail서버를 설치하는 경우 내부망에 설치하는 내부용 서버와 침입차단시스템 외부에 설치하는 외부용 서버를 서로 분리하여 운용하거나 이에 상응하는 적절한 보안대책을 수립한 후에 시행하여야 한다.

제16조(악성코드 방지대책) ① 연구원은 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호에 따라 정보통신시스템을 운영 관리하여야 한다.

1. 출처, 유통경로 및 제작사가 명확하지 않은 응용프로그램은 사용을 자제하고 불가피할 경우에는 백신 등 관련 검색프로그램으로 진단 후 사용
2. 익명으로 사용 가능한 서비스를 제한
3. 실행파일은 읽기 전용으로 속성 변경
4. 인터넷 등 상용통신망으로 입수한 자료는 반드시 악성코드 검색 후 사용
5. 악성코드 조기 발견을 위하여 최신의 검색프로그램 활용
6. 시스템이 작동할 때마다 컴퓨터 하드디스크의 부트섹터 및 메모리에 악성코드가 감염되었는지 검색

② 악성코드 감염이 발견되었을 경우에는 시스템관리자가 다음 각 호의 조치를 하여야 한다.

1. 악성코드 감염피해를 최소화하기 위하여 감염된 시스템 사용중지 및 내부망과 접속분리
2. 악성코드에 백신프로그램을 이용하여 악성코드 퇴치
3. 악성코드 감염확산 방지를 위하여 사용자에 관련 사실 및 보안조치사항 즉시 전달
4. 악성코드 감염의 재발을 방지하기 위하여 원인 분석 및 예방조치 수행

③ 연구원은 '사이버·보안진단의 날'을 이용하여 악성코드 감염여부를 진단토록 한다. 다만, 네트워크에 연결되어 자동 악성코드 체크 및 파일 업데이트가 되고 있는 PC는 그러하지 아니하다.

④ 연구원은 악성코드가 신종이거나 감염피해가 심각하다고 판단될 경우에는 관련사항을 보안담당자는 원장에게 신속히 보고하여야 한다.

제17조(보호구역 근무자 보안) ① 연구원은 정보통신실 등 보호구역에는 직원 외의 자를 통제하고 각 호의 보안조치를 수행해야 한다.

1. 보안의식 교육 및 별표4 서식에 의한 보안서약서 징구
2. 보안담당자 및 관계자에 대한 출입승인

② 원장 또는 보안담당자는 보호구역으로부터 전출 또는 퇴직자에 대해 다음 각 호의 보안조치를 수행해야 한다.

1. 전출 또는 퇴직자가 사용하던 PC에 저장되어 있는 비공개 자료 삭제
2. 전출 또는 퇴직자가 사용하던 사용자계정(ID)을 즉시 변경 또는 사용 중지

제18조(업무대행자 보안관리) ① 연구원은 정보시스템을 관리하기 위하여 일용직, 단순고용직 등을 업무대행자로 지정하여서는 아니 된다. 다만, 전문적인관리 업체를 지정할 경우에는 지정된 보안담당관의 승인 하에 지정하되, 다음 각 호의 사항을 준수하여야 한다.

1. 정보시스템의 접속시간, 접속 및 이용 권한을 최소화
2. 유효기간이 설정된 임시 접속계정 부여
3. 인가되지 않은 정보시스템에 불법 접속하는지 여부를 주기적으로 확인 점검

② 연구원이 제1항에 의하여 특정 정보시스템에 대해 업무대행자를 지정한 경우에는 다음 각호의 사항을 확인하는 등 보안조치를 수행하여야 하며, 그 사유가 소멸할 경우에는 즉시 해지하여야 한다.

1. 접속할 사용자, 사용자계정, 비밀번호
2. 접속주소, 접속시간, 접속사유(자료입력, 통계작성 등)
3. 접속 종료 후 사용자계정 및 비밀번호 회수 등 조치사항
4. 신원조사(기업 및 개인) 결과 또는 사본 비치

제19조(용역사업 준비단계 보안) ① 연구원은 정보화·정보보호사업 및 보안감리·보안컨설팅 수행 등을 외부 용역으로 추진할 경우에 연구원보완업무규칙에 따른 보안조치를 실시하여야 한다.

② 연구원은 제1항 관련 용역사업을 계약할 경우 계약서에 용역사업 참가직원의 보안준수사항과 위반할 경우에 손해배상 책임 등을 명시하여야 한다.

③ 연구원은 용역업체가 사업의 일부 또는 전부에 대하여 하도급 계약을 체결하는 경우에 용역업체로 하여금 하도급 계약서에 본 사업계약 수준의 비밀유지 조항을 포함하도록 조치해야 한다.

④ 연구원은 필요한 경우에 업무위탁 또는 용역인력을 대상으로 신원조사를 실시하여야 한다. 이 경우신원조사 대상자에 대한 조사결과를 고지하거나 누설행위를 금지하며, 업무상 직접적인 관련이 없이 신원기록을 열람하지 않도록 하는 등 신원조사 정보의 보안이 유지되도록 하여야 한다.

제20조(용역사업 수행단계 보안) ① 연구원은 용역사업의 참여인력에 대하여 별표4에 의한 보안서약서를 작성·제출토록 해야 한다.

② 연구원은 용역인력에 대해 비밀유지의 준수 의무 및 위반할 경우 처벌내용 등에 대한 보안교육을 실시해야 한다.

③ 연구원은 비밀관련 용역사업을 수행할 경우에 외부 참여인원에 대한 비밀취급인가 등 보안조치를 취해야 한다.

④ 연구원은 용역업체에게 자료를 제공하거나 용역수행 중 생산된 산출물에 대하여 다음 각 호에 따라 관리하여야 한다.

1. 비공개자료를 용역업체에게 열람하게 하거나 제공할 경우에 별표5의 열람·제공자료 관리대장으로 작성하여 인계자와 인수자가 직접 서명한 후 인수·인계 실시
2. 산출물 등 사업 관련자료는 인터넷 웹하드 등의 자료공유사이트 및 개인 메일함에 저장 금지, 대외비이상의 비밀은 전자우편으로 수·발신 금지
3. 용역업체에 제공한 비공개자료는 퇴근할 때 반납 조치하며, 비밀문서를 제외한 일반 문서는 시건장치가 된 보관함에 보관
4. 산출물 중 비공개 자료는 비인가자 또는 대외에 제공 또는 열람 금지

⑤ 연구원은 용역사업을 수행하는 사무실과 장비에 대하여 다음 각호에 따라 관리하여야 한다.

1. 시건장치가 구비되고 출입통제가 가능한 사무실 사용
2. 용역업체의 사무실과 인원·장비를 대상으로 정기적으로 보안점검 실시
3. 보호구역에서 용역사업자가 정보시스템이나 보조기억매체 등 정보자산을 반입 또는 반출하는 경우에 악성코드 감염 및 자료 무단반출 여부를 확인
4. 용역수행 PC에 허가받지 않은 USB 등 외부 저장매체 사용을 금지

제21조(용역사업 종료단계 보안) ① 연구원은 최종 용역산출물 중 대외보안이 요구되는 자료는 비밀, 대외비 또는 비공개자료로 등록하여 관리해야 한다.

② 연구원은 용역업체에 제공한 자료·장비·문서 및 중간·최종산출물 등 사업 관련 제반자료를 확인하여 전량 회수해야 하며, 노트북·보조기억매체 등에 의해 전자적으로 기록된 자료도 데이터 완전삭제 도구 등을 활용하여 복구가 불가능하도록 삭제 조치해야 한다.

③ 연구원은 제2항의 용역사업 관련자료 회수 및 삭제조치 후에 용역업체가 용역산출물의 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 용역업체 대표명의 별표6의 보안확약서를 작성·제출토록 해야 한다.

④ 연구원은 필요한 경우 용역사업에 투입된 PC 등에 대하여 제2항 및 제3항의 용역사업 관련자료 회수 및 삭제조치에 대한 이행여부를 확인할 수 있다.

제4장 경비 근무

제22조(책무) 연구원의 경비근무자는 청원경찰법 , 관계규칙 및 직무상의 명령을 숙지 준수하여 제반 근무상의 명령에 절대복종하여야 하며 근무기강을 확립하고, 연구원내의 각종사고 예방 및 질서를 유지하며 맡은바 책무를 성실히 수행하여야 한다.

제23조(근무시간 및 근무위치) 경비근무 시간은 연구원 근무명령에 의하여 근무하되 아래와 같이 실시한다.

① 경비의 근무시간은 09:00 ~ 18:00까지를 원칙으로 하며, 공휴일은 근무하지 않는다.

② 근무자는 별도의 지시가 있을 때까지 정문 경비실에서 계속근무하며 이상 유무사항이 있을시 행정경영실장에게 보고한다. 단 순찰근무 시에는 예외로 한다.

제24조(보고) 경비근무자는 근무 중 이상이 있을 때에는 즉시 행정실을 통하여 행정경영실장에게 보고한 다음 조치를 받아 별표7 경비근무일지에 기록 유지한다.

제25조(경비근무자의 임무)

1. 인원 및 차량통제
2. 물품의 반·출입 확인
3. 연구원내 시설물 확인(이상유무) 점검
4. 사고 예방활동(순찰)
5. 건물외곽청소 및 정리정돈
6. 경비근무일지 기록 유지
7. 기타 지휘계통에서 지시한 사항

제26조(준수사항) ① 경비근무자는 근무중 항상 지정된 장소에서 복장과 제장구를 단정히 착용하고 근무에 임한다.(근무복, 근무모, 혁띠 등)

② 근무중 근무지 무단이탈·음주·오락·투기행위·취침 등 경비근무자의 품위를 손상하거나 경비근무에 지장을 초래하는 행동을 하여서는 아니된다.

③ 경비근무자는 연구원의 표상임을 생각하고 외래객 방문시는 친절하게 안내 하여야 한다.

④ 경비근무자는 연구원 안전과 질서유지에 힘쓰고 이를 위반하는 자를 제재하고 즉시 관할 파출소에 연락하는 등 필요한 조치를 취하고 그 내용을 근무일지에 기록·보고 하여야 한다.

⑤ 근무상황부는 행정경영실장에게 매일 결재를 득하여야 한다.

제5장 비상상황대응

제27조(대응상황) 연구원 복무규정과 관련 공휴일 또는 시간외에 화재·도난·보안 기타 사고

의 예방과 긴급문서 처리 및 업무연락 등에 대응하기 위한 사항을 정한다.

제28조(정의) 이 장에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “총괄지휘자”이라 함은 연구원과 연구원이 점유 또는 소유하고 있는 부속재산의 비상상황 대응을 위한 총괄지휘·감독하는 자를 말한다.
2. “상황관리반장”이라 함은 비상대응총괄을 보좌하며 비상근무직원을 지휘하는 자를 말한다.

제29조(비상근무의 요령) ① 총괄지휘자는 연구원 및 연구원이 점유 또는 소유하고 있는 부속재산의 관리자를 미리 비상 근무반으로 편성하여 상황발생 시 자동적으로 근무에 임할 수 있는 체계를 갖추어야 한다.

② 비상근무 발령 중에는 소속직원의 소재를 항시 파악하여야 하며, 다음 각 호의 기준에 따라 근무하여야 한다.

1. 비상근무 1단계(경한사항)가 발령된 때에는 연가를 중지하고 부서별 현원의 10분의 1이상이 비상 근무한다.
2. 비상근무 2단계(중한사항)가 발령된 때에는 연가를 중지하고 부서별 현원의 5분의 1이상이 비상 근무한다.
3. 비상근무 3단계(중대사항)가 발령된 때에는 부득이한 경우를 제외하고는 연가를 억제하고 부서별 현원의 3분의1이상이 비상근무한다.

제30조(비상소집대상자지정운영) 원장은 비상상황대응을 신속하게 하기 위하여 별표8의 비상소집체계를 지정해야 한다.

제31조(응소자의 임무) ① 응소자는 비상연락을 받으면 지체없이 빠른 교통수단을 이용 등원하여 총괄지휘자 또는 상황관리반장의 지시에 의하여 근무에 임한다.

② 소집된 응소자는 부여받은 임무를 성실히 수행하여야 하며, 근무지를 무단이탈하지 못한다.

제32조(비상근무 제외자) 총괄지휘자 또는 상황관리반장은 비상근무에 있어서 부득이한 경우 일부직원에 대해 상황근무를 제외하게 할 수 있다.

제33조(비상근무 구성) ① 비상근무의 능률적인 수행을 위하여 상황관리반, 구조·구급반, 복구처리반을 두며, 각반의 임무는 다음 각호와 같다.

1. 상황관리반 : 피해상황 분석 및 상황보고서 작성 등 통제사항 서무에 관한 사항
2. 구조·구급반 : 인명구조, 대피로 확보 및 유도, 사상자 응급조치, 환자 후송등에 관한 사항
3. 복구처리반 : 2차 피해확산방지, 타 구조단 협조지원, 피해상황조사, 응급복구 및 주변정리 등에 관한 사항

② 제1항의 규정에 의한 상황관리반 편성은 다음 각 호와 같고 각 부서장이 반장이 된다.

1. 상황관리반 : 행정지원실에 둔다<개정 18.05.14>
2. 구조·구급반 : 연구개발본부에 둔다.<개정 18.05.14>
3. 복구처리반 : 전략기획본부, 신제품지원센터에 둔다.<개정 18.05.14><개정 21.06.30>

③ 상황관리반은 별표9으로 하며 대기자를 두어 교대하여 휴식하되 근무지를 이탈하거나 개별 행동을 지양하도록 한다.

④ 비상근무기간 중 필요한 차량을 대기시켜야 하며, 연구원차량을 비상상황 대기차량으로 한다.

제34조(상황실 설치) ① 비상소집 발령시 행정경영실은 비상근무상황실이 된다.

② 상황관리반은 비상근무상황실에서 비상상황에 대응할 수 있도록 각종 현황판을 설치하여 신속한 비상근무에 임하도록 한다.

제35조(비상상황대응 보고) ① 상황관리반은 상황이 종료될 때까지의 상황에 대하여 이사장 및 원장에게 다음 각 호의 사항을 수시 보고하여야 한다.

1. 비상상황의 개요 및 대응사항
2. 지도감독기관의 중요지시 내용 및 조치상황
3. 비상소집인원 및 비상근무현황

② 상황관리반은 비상소집명령 후 비상상황이 종료될 때까지 30분 간격으로 응소상황을 파악하여 기록유지하고 비상소집 종료와 동시에 그 상황을 이사장 및 원장에게 보고하여야 한다.

제36조(연락) 비상상황 대응의 연락은 문서, mobilephone문자, 이메일을 통한 연락매체를 활용하며, 그 내용을 기록 또는 출력 보관해야 한다.

제37조(직원연락체계의 유지) ① 연구원은 근무시간이 아닌 때에도 항상 소재파악이 가능하도록 연락체계를 유지하여야 한다.

② 연구원은 주소·전화번호 등 연락체계의 유지를 위하여 필요한 사항의 변경이 있는 때에는 이를 즉시 주관부서에 신고하여야 한다.

제38조(필수요원의 지정) ① 원장은 정상근무시간이 아닌 때에 긴급사태가 발생할 경우에 대비하여 소속직원 중 일부를 미리 필수요원을 지정하여 긴급사태 발생시 신속히 필요한 조치를 하도록 하여야 한다.

② 제1항의 필수요원은 비상소집 시 1시간이내에 응소가능한 자를 우선적으로 지정하되, 비상상황 대응이 가능한 인원을 위주로 지정해야 한다.

제39조(직원비상소집대상의 정비·보완) ① 원장은 직원비상소집 체계를 정비·보완하여야 하

며, 년 1회이상 이를 점검하여야 한다.

제6장 보 칙

제40조(보안관리) ① 원장은 연구원의 실·센터 주관으로 최종퇴청자가 해당 보안점검부 별표 10-1을 작성 관리 하도록 한다

② 삭제 <24.01.09>

③ 원장은 퇴직자에 대한 보안의무를 주지시키고, 퇴직자이행서약서 별표11 및 퇴직원 별표12을 징구해야한다.

제41조(통합열쇠관리) 원장은 사용자의 통합열쇠가 도용 및 불법복사 등을 방지하기 위해 다음 각 호 사항을 관리하여야 한다.

1. 통합열쇠 사용자 보안각서 별표13의 작성 절차를 거쳐 발급
2. 퇴직 또는 보직변경 등으로 사용자를 해지해야할 때에는 신속히 반납조치
3. 통합열쇠를 사용하고자 할 경우 행정경영실에 비치되어있는 통합열쇠대장 별표14에 기재 후 공용 통합열쇠 사용

부 칙

제1조(시행일) 이 규칙은 원장의 승인을 얻은 날부터 시행한다.

제2조(경과조치) 이 규칙 시행 이전에 행하여진 사항은 이 규칙에 의하여 시행 된 것으로 본다.

별표1.

보조기억매체(전산장비 포함) 반출·입 대장

장비명	관리번호 (S/N)	사용자 (직급)	용도	반출·입 일시 (반/출)	확인

별표2.

정보통신시스템 관리대장

연번	소속	취급자 (성명)	관리 번호	종류 (서버·PC 등)	비 밀 번 호 (필요시 장비용·사용자 인증용·자료용으로 구분)

※ PC 등의 비밀번호를 기재하지 아니할 수 있다.

※ 관리번호 : 각 부서별로 정보자산을 관리하기 위하여 부여하는 번호(예:10-8-1)

별표3.

IP주소 관리대장

부서	사용자명	IP Address	subnet mask	gateway	DNS Address	보조 DNS Address

별표4.

서 약 서

본인은 년 월 일부로 보안시스템과 관련한 업무(연구개발, 제작, 입찰, 기타)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 보안시스템과 관련된 소관업무가 연구원 사항임을 인정하고 제반 보안관계규정 및 규칙을 성실히 수행한다.

2. 본인은 이 기밀을 누설함이 이적행위가 됨을 명심하고 재직중은 물론 퇴직후에도 알게된 모든 기밀사항을 일체 타인에게 누설하지 아니한다.

3. 본인은 기밀을 누설한 때에는 아래 정부의 관계법규를 준용하여 엄중한 처벌을 받을 것을 서약한다.

   가. 국가보안법 제4조 제1항 제2호·제5호(국가기밀 누설 등)

   나. 형법 제99조(일반이적) 및 제127조(공무상 비밀의 누설)

   다. 군형법 제80조(군사기밀 누설)

   라. 군사기밀보호법 제9조(누설 및 제13조(업무상 누설)

년 월 일

서 약 자

소속 직급·직위

생년월일 성 명 인

별표5.

열람·제공자료 관리대장

사업명	자료명	인계 및 인수				자료반납	
		인계자	인수자	월일	장소	확인자	월일

297×210㎜(A4)

별표6.

보 안 확 약 서

본인은 귀 기관과 계약한 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 민·형사상책임과 손해배상을 감수하겠습니다.

년 월 일

서약업체(단체) 대표

소 속 :

직 위 :

성 명 : (서명)

ECO융합섬유연구원장 귀하

별표7.

경 비 근 무 일 지

담 당 자	업무총괄

▣ 20 년 월 일 (요일)

▣ 날씨 : , 온도 ℃

1. 순찰 상황

순찰 구역	점검 확인		세부 순찰 및 조치사항	방범, 방화, 소등, 누수 등
	오전	오후		
연 구 동				
공 장 동				
친환경연구센터				
창업보육센터				
건물 외곽 등				

2. 방문 상황

업체명 (성 명)	용 무	접견자

3. 임·직원 근무상황

성 명	시 간	내 용 (행선지 등)

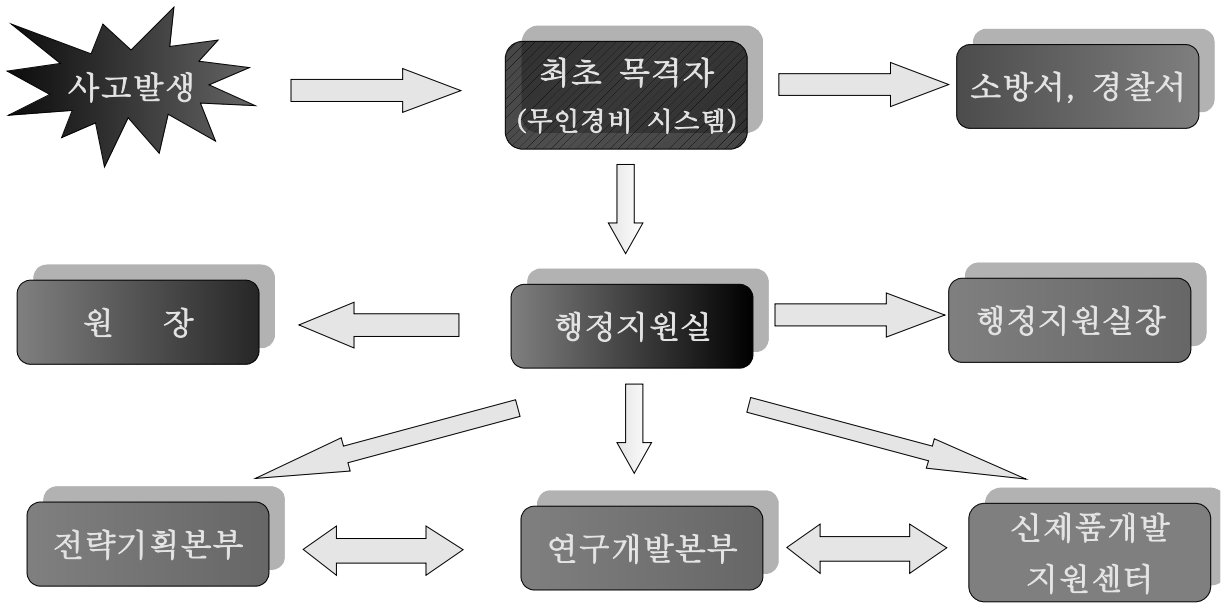
4. 우편,거래명세서 취급

구 분	연구원	입주업체
택 배	건	건
등기/우편	건	건
거래명세서	건	
기 타		

5. 기타 추진업무 상황

별표8. <개정 18.05.14><개정 21.06.30>

연구원 비상소집 체계도



□ 비상상황 보고

① 최초 목격자 : 행정지원실, 행정지원실장, 원장 보고
- 비상상황대응규칙 제35조(비상상황대응 보고) 준용
- 비상상황의 개요, 지도감독기관의 중요지시 내용, 비상근무현황 등

② 상황관리반 : 비상상황 내용 숙지 후 원장 및 행정지원실장 상황보고
- 비상상황대응규칙 제33조 (비상근무 구성)
· 상황관리반 : 내피해상황 분석 및 상황보고서 작성 등 통제사항 서무
· 구조·구급반 : 인명구조, 대피로 확보 및 유도, 사상자 응급조치 사항
· 복구처리반 : 2차 피해확산방지, 구조단 협조지원, 피해상황 조사 등

③ 상황 보고 후 지시에 따른 업무 연락 수행
- 비상상황의 대응사항, 지도감독기관의 내용 조치사항 전달

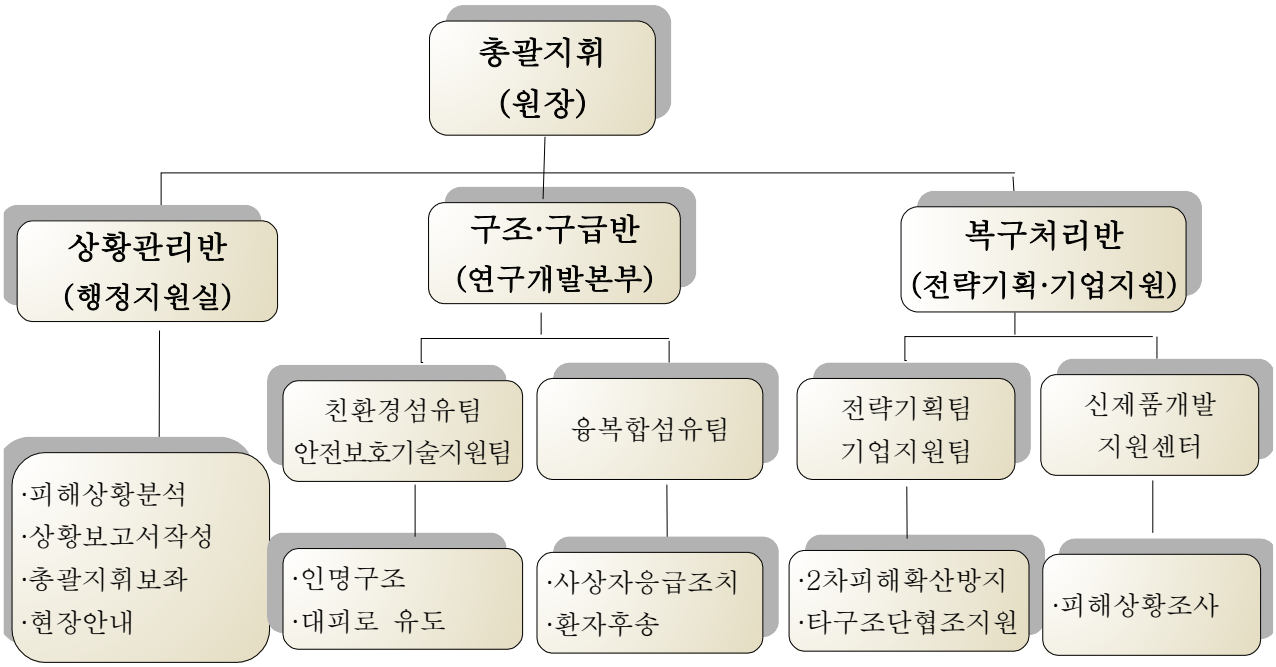
④ 필요부서(팀) 업무연락 통보

⑤ 해당 팀장은 업무연락을 받은 후 같은 본부(팀)의 전 부서원들에게 연락
- 비상상황대응규칙 제36조(연락) 준용
- 전화, 문서, SNS, 이메일 등 연락매체 활용 및 내용기록 보관

⑥ 필요시 상황관리반은 산업부, 전북도, 익산시 관련부서 상황보고

별표9. <개정 18.05.14><개정 21.06.30>

상황 조치 체계도



공통 조치

- 안전환경 체계에 따른 각 책임자의 사고원인 조사
- 사고원인 규명 및 재발 방지대책 수립 및 교육
- 자체 또는 외주업체 의뢰 현장복구 실시
- 사안에 따라 정부, 관련 유관기관에 보고

1) 비상 소집 후 1시간내 응소

2) 30분 단위 응소파악 및 상황보고

3) 상황 조치 체계도에 따른 각 팀장 또는 선임자가 업무 분장에 따른 조치 실시

4) 각 상황 대처상황을 상황관리반에 수시 보고

별표10-1.

보 안 점 검 부

점검일	서류보관 상 태	청소상태	소등상태	화기단속상 태	문단속상태	비 고	최 종 퇴청자		결 재
							점검 시간	성 명	실 장

별표10-2. <삭제 24.01.09>

별표11.

퇴직자 이행 서약서

본인은 201 . . .부로 퇴직함에 있어서 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인이 연구원에 재직한 기간 중 업무 수행과 관련하여 지득(知得)한 기밀은「정관」「제반규정」「제반규칙」특히「ECO융합섬유연구원 업무노트 작성·관리규정」에 의거 보완 및 기밀유지 의무에 따른다.

2. 본인은 이 기밀에 대하여 재직 중은 물론 퇴직 후에도 지득(知得)한 제반 비밀사항을 일체 누설하지 않을 것을 서약한다.

3. 본인이 이 기밀을 누설한 때에는 동기여하를 막론하고 그 결과가 연구원의 손실 행위임을 자인하며, 민·형사상의 책임을 지고 엄중한 처벌을 받을 것을 서약한다.

20 년 월 일

서 약 자 소속부서 :

직위·직급 :

성 명 : (인)

ECO융합섬유연구원 귀하

별표12.

퇴 직 원

1. 소속부서 :

2. 직위·직급 :
(상당계급)

3. 성 명 :

위 본인은 일신상 이유로 자유의사에 따라 퇴직코자 하오니 허락하여 주시기 바랍니다.

년 월 일

신청인 (서명 또는 인)

ECO융합섬유연구원장 귀하

별표13.

통합열쇠 사용자 보안각서

주　　소 :

성　　명 :

생 년 월 일 :

상기 본인은 ECO융합섬유연구원 통합열쇠를 관리함에 있어 절대로 타인에게 대여하지 않는 것을 원칙으로 하되 불가피하게 대여했을 경우 발생되는 보안상의 문제(분실, 훼손)시 전적으로 본인이 책임지며, 어떠한 이의도 제기치 않을 것임을 각서 한다.

20　년　월　일

각 서 인 :　　(인)

ECO융합섬유연구원장 귀하

별표14.

통 합 열 쇠 대 장

연 번	부 서	일 시	성 명	사 용 목 적	확 인	비 고