

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	1 / 24

## 목차


제 1 장. 총칙	5
제 1 조. (정보보호 원칙)	5
제 2 조. (정보보호 정책 운영 체계)	5
제 3 조. (적용범위)	5
제 4 조. (정보보호 대상)	5
제 5 조. (책임과 역할)	6
제 6 조. (정보보호 요구사항)	6
제 2 장. 정보보호 규정	6
제 7 조 (정보보호 규정 수립 및 공표)	6
제 8 조 (정보보호 규정 준수)	7
제 9 조 (정보보호 규정 관리)	7
제 10 조 (정보보호 규정의 제·개정)	7
제 3 장. 정보보호 조직	8
제 11 조 (정보보호 조직의 구성)	8
제 12 조 (조직 구성 기준)	8
제 13 조 (정보보호위원회 운영)	8
제 4 장. 개인정보 보호	9
제 14 조 (개인정보 보호책임자 지정)	9
제 15 조 (개인정보보호 업무의 운영)	9
제 5 장. 인적보안	9

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	2 / 24


제 16 조 (정보보호 서약 및 갱신)	9
제 17 조 (전입 및 채용)	9
제 18 조 (전출 및 퇴사)	10
제 19 조 (인력 보안관리)	10
제 20 조 (교육 프로그램)	10
제 21 조 (상벌제도)	10
제 22 조 (외주용역 추진 시 검토사항)	11
제 23 조 (계약 시 보안대책)	11
제 24 조 (업무 수행 시 보안대책)	11
제 25 조 (업무 완료 시 보안대책)	12
제 6 장. 정보자산 관리	12
제 26 조 (정보자산의 식별 및 관리)	12
제 27 조 (중요 정보의 분리)	12
제 28 조 (정보자산 등급 분류 및 표시)	13
제 29 조 (정보자산 등급별 관리)	13
제 7 장. IT 인프라 보안	14
제 30 조 (사용자 인증 및 식별)	14
제 31 조 (사용자 계정 관리)	14
제 32 조 (패스워드 관리)	14
제 33 조 (로그 관리)	14
제 34 조 (백업 및 소산 관리)	15
제 35 조 (시스템 보안)	15

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	3 / 24

제 36 조 (데이터베이스 보안)	15
제 37 조 (침입차단시스템(방화벽))	15
제 38 조 (웹 보안)	16
제 39 조 (네트워크 운영)	16
제 40 조 (임직원 계정의 변경 및 삭제)	16
제 41 조 (외부에서 내부 네트워크로의 접근)	16
제 42 조 (인터넷 및 네트워크 사용)	17
제 43 조 (바이러스 관리)	17
제 44 조 (PC 관리)	17
제 45 조 (계정 관리)	18
제 8 장. 모바일기기 보안	18
제 46 조 (모바일기기의 정의)	18
제 47 조 (모바일기기 보안 관리 업무의 운영)	18
제 9 장. 물리 보안	19
제 48 조 (보호구역의 구분)	19
제 49 조 (보호구역 접근통제)	19
제 50 조 (전산장비 보안)	19
제 51 조 (전산 시설 보호)	19
제 52 조 (사무실 보호 대책)	19
제 10 장. 개발보안	20
제 53 조 (적용 범위)	20
제 54 조 (개발보안 관리 업무의 운영)	20

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	4 / 24

제 55 조 (외주개발 계약)	20
제 56 조 (외주개발 관리 및 검수)	20
제 57 조 (소프트웨어 개발보안)	20
제 11 장. 위험평가	21
제 58 조 (위험관리)	21
제 59 조 (위험평가 업무의 운영)	21
제 12 장. 보안사고 대응	21
제 60 조 (보안사고의 예방 및 대응)	21
제 13 장. 보안 점검 및 감사	21
제 61 조 (보안 점검 및 감사 준수 관리)	21
제 62 조 (점검 및 감사 결과의 처리)	22
제 14 장. 업무 연속성	22
제 63 조 (업무 연속성 계획 수립)	22
제 64 조 (업무 연속성 계획 가동)	22
제 65 조 (업무 연속성 사후관리)	22
부 칙	23

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	5 / 24

## 제 1 장. 총칙

### 제 1 조. (정보보호 원칙)

㈜세아홀딩스(이하 '회사'라고 함)는 정보보호 국제표준과 국내외 관련 법률을 준수하고 핵심기술 등의 정보자산을 보호하여 글로벌 경쟁력 확보와 유지에 최선을 다하며, 이를 위해 정보보호에 대한 공정하고 합리적인 정책과 기준을 마련하고 임직원 및 외부 이해관계자 모두가 정보보호의 생활화를 통해 실행력을 확보하여 최고수준의 정보보호 상태를 유지하도록 노력하여야 한다.

### 제 2 조. (정보보호 정책 운영 체계)

회사는 정보보호 원칙을 기반으로 정보보호 규정 및 지침을 제정하여 시행하며, 매년 최신 법률과 제도, 대내외 환경을 반영하여 해당 규정 및 지침을 개정한다. 규정과 지침의 제. 개정 및 폐지 시 정보보호 최고 책임자(이하 'CISO'라고 함)가 검토하여 최고경영진에 보고 후 승인을 받아 확정한다. 정보보호 규정 및 지침 문서는 모든 임직원이 열람할 수 있도록 게시하여야 한다.


정보보호 정책 체계는 원칙, 규정, 지침의 3 단계로 구성되어 있으며, 필요에 따라 정보보호 지침의 하부에 운영기준을 명시하여 실행부서 주관으로 운영한다. 운영기준에는 프로세스 절차를 포함한다.

### 제 3 조. (적용범위)

본 규정은 회사가 보유하고 있는 모든 정보자산을 대상으로 하며, 전 임직원 및 회사의 업무에 종사하는 외부회사 임직원 등을 포함하여 적용한다.

### 제 4 조. (정보보호 대상)

1. 정보보호의 대상은 회사의 정보자산으로 한다. 정보자산은 정보와 정보시스템으로 구분되며, 이를 운영하기 위하여 필요한 정보 관련 자산 역시 정보보호의 대상이 된다.
2. 정보는 회사 임직원들이 경영활동과 관련하여 생성 또는 입수하여 소유하고 있는 지적 자산 등 컴퓨터나 저장매체에 기록된 정보와 각종 인쇄물 등을 포함한다.
3. 정보시스템은 회사가 사용 또는 관리하는 모든 하드웨어, 소프트웨어, 네트워크 등을 포함한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	6 / 24

4. 정보자산은 사업을 수행하기 위해 꼭 필요한 정보는 물론 그 정보를 만들거나 보관, 전송하는 장치 또는 시설물, 기록문서, 인쇄물, 도면, 정보시스템 등 모든 유·무형의 물질을 포함한다.

### 제 5 조. (책임과 역할)

1. 정보시스템을 통하여 생산, 저장, 전송, 처리되는 정보와 이에 의하여 제공되는 정보서비스는 회사의 중요한 자산이다.
2. 임직원, 외부업체 직원은 본 규정을 이해하고 준수함으로써 회사의 정보자산을 보호할 책임이 있다.
3. 임직원 및 외부업체 직원은 정보자산을 자연재해, 시스템 및 네트워크의 고장, 내·외부 인원에 의한 우발적이거나 의도적인 각종의 위협으로부터 보호해야 한다.

### 제 6 조. (정보보호 요구사항)


회사의 정보자산은 다음과 같은 요구사항을 충족하여야 한다.

- (1) 정보자산의 접근은 인가된 사람만이 접근 가능함을 보장하여야 한다.
- (2) 정보자산 내의 정보 및 처리 방법의 정확성, 완전성을 보호하여야 한다.
- (3) 인가된 사용자가 필요시 정보자산 및 관련 정보에 접근하는 것을 보장하여야 한다.

## 제 2 장. 정보보호 규정

### 제 7 조 (정보보호 규정 수립 및 공표)

1. CISO 는 전 임직원이 준수하여야 할 정보보호 기본 방침을 포함하는 정보보호 규정과 구체적 시행을 위한 세부지침을 수립하여 운영하여야 한다.
2. 정보보호 담당자는 승인을 득한 정보보호 규정 및 지침을 회람, 게시 등 적절한 방법으로 전 임직원 및 관계된 모든 인원들이 인식할 수 있도록 공표한다.
3. 정보보호 규정 및 지침 문서는 원칙, 적용범위, 역할 및 책임, 운영체계 등을 명시하여야 하며 개정이력을 관리하여야 한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	7 / 24

## 제 8 조 (정보보호 규정 준수)

1. 전 임직원 및 외부인력은 정보보호와 관련된 회사의 정보보호 규정, 지침 및 운영기준 등을 준수하여야 한다.
2. 임직원이 회사의 정보보호 규정 및 세부지침을 위반하여 회사에 재산상의 손실을 입히거나 이미지를 훼손한 경우에는 내규에 따라 징계할 수 있다.
3. 회사와 계약관계에 있는 제 3 자가 회사의 정보보호 규정 및 지침을 위반하거나 보안사고가 발생한 경우에는 관계기관과 협조하여 원인을 규명하고 관련법에 따라 조치한다.

## 제 9 조 (정보보호 규정 관리)

CISO 는 정보보호관리체계의 적절성 및 준수를 보장하기 위해 정보보호 규정 및 세부지침에 대하여 다음 각 호의 사항을 연 1 회 이상 검토하고 반영하여야 한다.

- (1) 정보보호 환경의 중요한 변화 발생
- (2) 새로운 위협 또는 취약점 발생
- (3) 조직 및 임무 등의 대대적인 변경 발생
- (4) 자산에 대한 위험평가 프로세스에 영향을 주는 변화 발생
- (5) 중대한 침해사고 발생
- (6) 정보보호관리체계 상의 중대한 결함 발생
- (7) 회사 사업 환경에 대한 중대한 변화 발생
- (8) 정보보호 규정 및 세부지침의 효과성 및 일관성
- (9) 그 외 경영진에서 필요하다고 인정할 경우

## 제 10 조 (정보보호 규정의 제·개정)

1. 정보보호 관리자는 정보보호 규정 및 지침의 검토 결과 제·개정이 필요한 경우 다음 절차에 따르며, 검토결과, 제·개정, 배포, 폐기 등에 대한 이력을 기록·관리하여야 한다.
  - (1) 정보보호위원회 구성원의 제정 및 개정 필요성 분석
  - (2) 정보보호 담당자 및 해당 실무자의 검토
  - (3) 개정안 작성, CISO 또는 정보보호 담당자의 검토
  - (4) 정보보호 관련 절차 전결권자 승인

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	8 / 24

- (5) 제·개정된 규정/지침/운영기준 공표 및 교육
- (6) 제·개정된 규정/지침/운영기준 적용 및 준수
2. CISO는 정보보호 규정 및 지침의 제·개정 의무에 대한 이행 기록 및 제·개정, 폐지에 대한 검토 기록은 유지 및 보관하여야 한다.
3. 최고경영진은 해당 규정·지침·운영기준을 확인하고 최종 승인한다.

## 제 3 장. 정보보호 조직

### 제 11 조 (정보보호 조직의 구성)

회사는 정보보호 관련 업무를 담당하는 정보보호 조직을 운영하며, 정보보호 관리자 및 정보보호 담당자를 지정하여 정보보호활동 실무에 대한 관리를 수행한다.


### 제 12 조 (조직 구성 기준)

1. 회사의 정보보호 조직은 다음과 같이 구성한다.
  - (1) 정보보호 최고 책임자(CISO)
  - (2) 정보보호 관리자
  - (3) 정보보호 담당자
  - (4) 정보처리시스템 담당자
2. 회사의 정보보호 조직은 인사발령에 의하며, 각 구성원은 책임과 역할에 대한 명확한 인지를 하여야 한다.

### 제 13 조 (정보보호위원회 운영)

1. 회사의 전반에 걸친 중요한 정보보호 관련사항에 대해 검토 및 의사결정을 할 수 있는 정보보호위원회를 구성하여야 한다.
2. 정보보호위원회의 위원은 다음과 같이 구성한다.
  - (1) 위원장: 정보보호 최고 책임자(CISO)
  - (2) 간사: 정보보호 관리자, 정보보호 담당자
  - (3) 위원: 유관부서의 팀장



	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	9 / 24

- 정보보호위원회는 조직 전체의 정보보호 정책 목표, 목적 및 우선순위 등을 고려하여, 연 1 회 이상 회사의 정보보호 주요 현안을 검토하고 이에 대한 의사결정을 수행한다.

## 제 4 장. 개인정보 보호

### 제 14 조 (개인정보 보호책임자 지정)

개인정보 보호책임자 (이하 CPO – Chief Privacy Officer'라 칭함)는 개인정보보호 업무를 주관하는 임원으로 최고경영자(CEO)가 지정한다.

### 제 15 조 (개인정보보호 업무의 운영)

개인정보와 관련된 규정은 '개인정보 보호지침'을 통하여 준수하도록 하고 개인정보 업무와 관련된 세부사항은 '개인정보 내부관리계획'을 수립하여 따르도록 한다.


## 제 5 장. 인적보안

### 제 16 조 (정보보호 서약 및 갱신)

- 임직원은 입사 및 퇴사 시 회사의 정보보호 정책을 이해하고, 이를 준수하겠다는 내용의 동의 및 서약을 징구하며, 별도의 기준을 마련하여 주기적으로 갱신하여야 한다.
- 정보보호 서약서에는 다음의 내용이 포함되어야 한다.
  - 회사 정보보호 정책의 준수
  - 영업비밀 및 개인정보보호법에 준하는 개인정보의 보호
  - 기타 회사와 관련된 법규 및 요건에 대한 준수
  - 정보보호 관련 법령에 대한 준수
  - 위반시의 책임 감수

### 제 17 조 (전입 및 채용)

- 인사 담당자는 인력의 전입 및 채용 시 이력서 점검, 학력, 경력 및 신원의 확인을 수행한다. 특히 중요 정보 취급자일 경우 사전에 업무의 적격성을 충분히 검토한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	10 / 24

- 인사 담당자는 임직원의 전입 및 채용 시 임직원으로 하여금 회사 정보보호에 대한 책임을 이해하고 이를 준수하겠다는 내용의 동의 및 서약서에 서명하도록 하며, 명시된 기밀 준수 사항을 반드시 지키도록 한다.
- 신규 입사자에 대한 교육은 정보보호팀이 주관하여 정보보호 규정 및 정보보호에 대한 교육을 실시한다.

### 제 18 조 (전출 및 퇴사)

인사 담당자는 임직원의 전출 또는 퇴사시 정보보호 서약서를 징구하고, 지원 담당자는 보유중인 회사의 모든 정보자산 및 정보시스템 사용권한, 사원증 등을 회수하여 개인 물품 이외의 반출이 불가하도록 하여야 하며 정보보호 관리자는 퇴사 프로세스 상에서 보안관련 절차(권한회수 등)를 준수하였는지 확인 하여야 한다.

### 제 19 조 (인력보안 관리)


- 정보보호담당자 및 인사담당자는 인사 변경 발생 시 정보자산 반납, 접근권한의 변경 및 회수 조치가 신속하게 이루어질 수 있도록 인사 변경 사항을 회사 내에 공유하여야 한다.
- 기타 인력 보안의 세부적인 사항에 관하여는 '인적보안 지침'에 따른다.

### 제 20 조 (교육 프로그램)

- 정보보호 교육은 교육대상, 교육자원(인력, 예산 등, 교육방법 및 주기) 등을 고려하여 계획하여야 한다.
- 신규 입사자에 대해 부서 배치 전 회사의 정보보호 정책 및 업무상 필요한 정보보호 활동을 주지시키기 위해 정보보호 교육을 실시할 수 있다.

### 제 21 조 (상벌제도)

임직원의 정보보호 인식제고 및 정책의 준수를 위하여 상벌제도를 운용할 수 있으며, 이를 위한 징계 기준을 수립하고 적용하여야 한다

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	11 / 24

## 제 22 조 (외주용역 추진 시 검토사항)

주요 정보시스템의 개발 및 운영업무를 외주용역으로 대체하는 경우 보안관리의 취약점을 최소화하고 정보보호를 위하여 내부 통제방안을 수립 및 운영하여야 한다.

## 제 23 조 (계약 시 보안대책)

1. 정보보호 및 개인정보보호 역량이 있는 업체가 선정될 수 있도록 관련 요건을 제안요청서(RFP) 및 제안 평가항목에 반영하여 업체 선정 시 적용하여야 한다
2. 외부업체 혹은 외부인력과 위탁 계약 시 계약서에는 보안 요구사항과 보안위험 및 보안대책에 대한 요구사항을 명시하여야 한다.
  - (1) 비밀유지, 정보보호 준수 의무, 보안사고 발생 시 책임
  - (2) 정보보호 활동에 대한 보고 및 승인
  - (3) 정보보호 활동에 대한 모니터링 및 감사권한
  - (4) 정보보호 관련 상호책임

## 제 24 조 (업무 수행 시 보안대책)

1. 외부인력의 업무 수행에 관련된 보안 관리는 정보보호담당자가 관리·감독한다.
2. 외부인력과 업무 수행 시 보안 정책의 준수와 비밀 유지에 대한 정보보호서약서를 별도 징구 하여 관리한다.
3. 외부인력이 업무 수행을 위한 공간을 제공한 후 물리적 보안을 적용하여 출입을 엄격히 통제한다.
4. 외부인력의 활동에 대한 정보보호 규정은 기본적으로 임직원에게 대한 정보보호 규정에 준한다.
5. 외부인력에 대해 주기적으로 점검하여 보안 위반사항이 없는지 확인하며, 발견된 문제점에 대하여 개선계획을 수립·이행하여야 한다.
6. 외부인력의 정보보호 정책 위반 시, 그 결과를 해당 업체에 경고 조치하고, 계약에 따른 해지, 손해배상 등의 필요 조치를 수행하여야 한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	12 / 24

## 제 25 조 (업무 완료 시 보안대책)

1. 담당조직은 외부자의 업무 종료 또는 계약 완료, 담당자 변경이 발생했음을 신속하게 인지할 수 있도록 정보를 공유하고, 각 정보보호담당자는 접근권한 등이 완전히 삭제되었는지, 불필요한 정보들이 유출되지 않는지 등을 점검 후, 정보보호 서약서를 징구하여야 한다.
2. 외부인력에게 제공한 회사 소유의 모든 정보자산을 회수하며, 개인 PC, 노트북, 저장장치 등에 포함된 회사의 지적재산과 관련된 모든 정보는 삭제해야 한다.


## 제 6 장. 정보자산 관리

### 제 26 조 (정보자산의 식별 및 관리)

1. 회사의 모든 정보자산은 식별되고, 식별된 정보자산에 대해서 목록을 작성하여 이를 연 1 회 이상으로 검토하여 최신성을 유지하여야 하며, 자산이 변동되는 경우 1 개월내 변동 내역을 자산 목록에 반영해야 한다.
2. 정보자산이 인사이동(퇴직, 전보 등) 및 신규로 발생하는 경우 정보자산 소유자는 해당 자산을 정보자산목록에 등록해야 한다.
3. 식별된 정보자산에 대한 실제 관리·운영하는 관리자 또는 담당자를 지정하여 책임소재를 명확하게 하여야 한다.
4. 정보자산의 등급은 정보를 최초 생성하는 정보의 소유자와 정보보호담당자가 정보의 중요도에 따른 적절한 수준의 보호를 하기 위하여 정보의 등급을 결정하고 그에 따른 보호 방법을 명시해야 한다.

### 제 27 조 (중요 정보의 분리)

1. 회사의 정보자산은 그 중요도에 따라 "비공개", "대외비", "비공개대외비"등 3 단계로 분류한다.
  - (1) "비공개대외비"란 주로 경쟁사 및 대외로 유출될 경우 기업 활동에 중대한 영향을 미쳐 회사가 막대한 손해를 입을 수 있는 정보를 말한다. 여기에는 회사 업무상 중요하게 취급되는 인사, 급여 등의 정보를 포함한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	13 / 24

(2) "대외비"란 경쟁사 및 대외로 유출될 경우 회사에 피해를 줄 수 있는 정보 중 "비공개대외비"에 해당하지 않는 것을 말한다.

(3) "비공개"란 내부 결재권자 외 내부에 유출될 경우 업무상 혼란을 미칠 수 있는 정보를 말한다

2. 자산의 분류는 일정 기간마다 새롭게 지정·변경 및 해제가 가능하다.

### 제 28 조 (정보자산 등급 분류 및 표시)

1. 회사의 정보자산에 대한 중요도를 평가하여 보안 등급별로 분류하고 정기적으로 적정성을 검토하여야 한다.
2. 문서, 저장매체 등에는 회사 기준에 따라 보안 등급을 표시하고 관리하여야 한다.
3. 데이터 저장소상에서 생성 및 관리되는 정보자산 (디지털 저작물)도 동일한 회사 기준에 따라 3 단계 분류기준에 따라 Label 이 자동 설정되도록 한다.


### 제 29 조 (정보자산 등급별 관리)

1. 정보자산은 보안 등급에 따라 취급절차(생성, 저장, 이용, 파기 등)수립 및 사용자를 지정하고 비인가자의 접근을 차단하여야 한다.
2. 중요 정보자산에 대해서는 주기적으로 보안점검 및 분석을 수행하고 발견된 취약점에 대해서는 통제대책을 강구하여야 한다.
3. 중요 자료 및 문서 등의 폐기시에는 해당 내용을 복구할 수 없도록 파기 또는 완전 삭제 등을 시행하여야 한다.

## 제 7 장. IT 인프라 보안

### 제 30 조 (사용자 인증 및 식별)

임직원, 협력업체 직원, 임시직원 등의 사용자를 대상으로 어플리케이션, 서버, 네트워크 장비, DB 등의 정보시스템 접속 시 인증을 통해 필요한 최소의 권한만을 부여 받도록 함으로써 인가되지 않은 사용자의 접근 및 정보의 사용을 통제하는데 그 목적이 있다. 정보시스템의 인증 구현 시 사용자 및 업무의 중요도, 접근 과정에 따른 위험, 자원의 중요성 등을 고려하여 인증 방식을 차등 적용하여야 한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	14 / 24

### 제 31 조 (사용자 계정 관리)

정보시스템 계정(ID)의 등록, 변경, 삭제 등에 대한 관리 기준을 수립하고 유지해야 하며, 변경 이력을 보관하여야 한다.

### 제 32 조 (패스워드 관리)


1. 패스워드는 연속된 숫자, 아이디 포함을 제한하고, 생일, 전화번호 등 추측하기 쉬운 문자열을 사용을 지양하며, 영문자, 숫자를 포함하여 2 종류 조합 10 자리 이상 또는 영문자, 숫자, 특수문자를 조합하여 3 종류 8 자리 이상 설정하여야 한다.
2. 임직원이 패스워드를 사용할 수 있는 최대 기간은 3 개월(분기)로 한다. 단, IT 인프라 운영에 직접적인 영향을 미치는 계정으로 정보보호 관리자에게 인정될 경우 또는 시스템 운영 상 차질 등으로 인해 별도 요청이 있을 경우 정보보호담당자의 판단 하에 변경주기에 대한 기간을 변경할 수 있다.
3. 패스워드 5 회 실패 시 계정이 잠기도록 임계치를 설정하여야 한다.

### 제 33 조 (로그 관리)

1. 모든 시스템의 로그기능은 반드시 활성화시키고, 로그내역에 대해서는 불법 수정되지 않도록 보호한다.
2. 정보보호 담당자는 침해시도, 침해상황 등을 포함한 로그분석 결과를 문제 발생 시 정보보호 관리자에게 보고한다.

### 제 34 조 (백업 및 소산 관리)

1. 세부 주기와 방법에 대한 별도의 절차를 마련하여 소프트웨어 및 데이터의 유실방지를 위해 정기적으로 백업을 실시한다.
2. 백업일자, 대상, 소유자, 작업자, 보관장소 등이 기록되어 있는 백업목록을 기록 유지하여야 한다.
3. 저장된 데이터의 중요도에 따라 백업매체를 분류하고 분류에 따라 라벨링을 수행하여야 한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	15 / 24

- 백업매체에 대해서는 보안을 강화하고 필요 시 재해를 대비하여, 시건 장치가 되어 있는 안전한 장소에 소산하여 보관할 수 있다.

### 제 35 조 (시스템 보안)

- 시스템의 안정화와 보안을 위해 점검 및 예방활동을 수행하여야 한다.
- 모든 시스템은 알려진 보안취약성을 제거한 후 업무망에 연결하여야 한다.
- 주기적으로 시스템에 대한 보안상태를 점검하고, 패치를 실시하는 등의 시정조치를 취하며, 그 결과를 정보보호 관리자에게 보고한다.

### 제 36 조 (데이터베이스 보안)


- 데이터의 정확성을 유지하기 위해서 데이터의 수정, 변경 등은 로깅이 가능한 어플리케이션을 통해서만 수행하고 데이터베이스의 직접적인 수정을 금한다.
- 데이터베이스의 데이터는 백업 정책에 의거하여 주기적으로 백업한다.
- 데이터베이스 접근에 대한 감사기록을 유지하며, 일반 사용자들은 감사기록을 접근하지 못하도록 한다.
- 기밀 데이터는 데이터베이스 저장 시 암호화하거나 권한 없는 자가 조회할 수 없도록 특별한 대책을 수립하여야 한다.

### 제 37 조 (침입차단시스템(방화벽))

- 외부로부터의 모든 접속은 침입차단시스템을 경유한다.
- 외부에서 내부로의 모든 접속시도는 침입차단시스템에서 로그를 쌓아 관리되어야 한다.
- 침입차단시스템의 정책변경은 엄격히 통제되어 설정하여야 하며, 별도의 절차를 수립하여 운영하여야 한다.

### 제 38 조 (웹 보안)

- 공개 웹 서비스가 제공되는 시스템에서는 대외비 이상의 정보가 게시되어서는 아니 된다.
- 관계사 간 주요 정보가 웹 서비스를 통해 인터넷 상에서 교환될 경우 SSL 등의 암호화를 적용하여 전송내용을 보호한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	16 / 24

3. 웹 서버에 대해서는 침입탐지 대책을 적용하고, 불필요한 서비스가 운영되지 않도록 하고, 주기적으로 패치를 설치하며, 보안 취약성 점검을 수행하고 이에 따른 대책을 운영한다.

### 제 39 조 (네트워크 운영)

1. 네트워크의 안정화와 보안을 위해 점검 및 예방활동을 수행하여야 한다.
2. 주기적으로 네트워크 연결에 대한 보안상태를 점검하고 그 결과를 정보보호관리자에게 보고하여야 한다.

### 제 40 조 (임직원 계정의 변경 및 삭제)

1. 정보처리 시스템 담당자는 IT 인프라 설치 시 기본적으로 포함되어 있는 제품 공급 계정 중 업무적으로 불필요한 계정을 삭제하여야 한다.
2. 정보처리 시스템 담당자는 3개월 이상 임직원 계정이 사용되지 않을 경우 해당 계정의 접근을 차단한다.
3. 정보처리 시스템 담당자는 퇴사 및 인사변동 사항을 인사담당자로부터 제공받아 해당 임직원의 계정을 즉시 삭제 또는 접근을 차단한다.
4. 정보처리 시스템 담당자는 불필요한 계정 및 미 사용계정에 대하여 정보보호담당자 및 관리자가 요청 시 해당 계정에 대하여 권한 회수 및 계정삭제 처리를 실시한다.

### 제 41 조 (외부에서 내부 네트워크로의 접근)

1. 외부에서 내부 네트워크로 접속할 경우 관리자 권한으로 로그인하는 것은 허용하지 않는다. 또한 외부에서 내부 네트워크로 접속한 경우 접속기록에 대한 로깅을 실시한다.
2. 외부에서 임직원이 내부 시스템에 접속하려면 VPN 등의 강화된 인증 및 암호화를 적용하고 이에 대한 접속기록에 대해 로깅을 실시한다.

### 제 42 조 (인터넷 및 네트워크 사용)

1. 공개된 장소에서 인터넷으로 회사 내부의 시스템에 접속하는 것을 금지한다.
2. 인터넷으로부터 함부로 파일을 다운로드 받지 않는다. 파일을 다운로드 받을 경우 백신소프트웨어 등을 통해 반드시 바이러스 점검을 거친다.



	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	17 / 24

- 개인정보 침해 방지를 위해 무분별한 사이트 가입을 지양하고 최대한 자신의 정보를 노출하지 않는다.

### 제 43 조 (바이러스 관리)

- 모든 서버 및 PC 에 대해 바이러스 검색 및 치료 프로그램을 설치한다.
- 바이러스 검색 및 치료 프로그램은 항상 최신의 정보를 포함하도록 자동적으로 업데이트하는 절차를 마련하여야 한다.
- 전자우편의 첨부파일에 대해서는 반드시 바이러스 검사를 한 후 사용한다.

### 제 44 조 (PC 관리)

- PC 부팅 및 로그인 시 패스워드를 설정하여 비 인가자의 접근을 방지한다.
- 자리 이석 시 비 인가자의 불법적인 사용을 방지하기 위해, 화면보호기를 설정하고 대기시간은 10 분 이내로 패스워드를 설정한다.
- 기밀 정보를 PC 에 저장할 경우 암호화를 하여 저장하여야 한다.
- 정보보호 담당자는 주기적(반기 1 회)으로 부서 내에 보유하고 있는 PC 에 대한 보안 점검을 실시한다.

### 제 45 조 (계정 관리)

- 계정신청은 계정신청 절차에 따라 신청 및 승인 후 사용할 수 있다.
- 임직원 계정은 개인별 부여 및 관리하여야 하며, 공용 계정은 사용하지 않는 것을 원칙으로 한다.

## 제 8 장. 모바일기기 보안

### 제 46 조 (모바일기기의 정의)

“모바일기기”라 함은 업무용으로 사용하기 위하여 회사가 구입하여 임직원에게 제공된 스마트폰, 태블릿 PC 등과 같은 일체의 기기 혹은 회사의 명의로 회선을 개통하고 해당 회선을 이용하고 있는 스마트폰, 태블릿 PC 등의 기기를 의미한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	18 / 24

### 제 47 조 (모바일기기 보안 관리 업무의 운영)

모바일기기 보안 관리 업무의 운영과 관련된 세부사항은 '모바일기기 보안지침'을 따른다.

## 제 9 장. 물리 보안

### 제 48 조 (보호구역의 구분)

1. 회사 내 정보보호 상 제한과 통제가 요구되는 지역(시설)은 보호구역으로 설정하며, 중요도에 따라 "통제구역", "제한구역", "일반구역"으로 구분·적용하여 관리하여야 한다.
2. 보호구역의 세부적인 사항에 관하여는 '물리보안 지침'에 따른다.

### 제 49 조 (보호구역 접근통제)

보호구역에 대한 출입 및 감시 기록을 유지하여야 하며, 주기적으로 권한 및 운영의 적정성을 검토하여야 한다.

### 제 50 조 (전산장비 보안)


전산장비 설치 시에는 불필요한 접근 및 위험을 최소화하도록 배치하고 필요한 통제수단을 도입하여야 한다.

### 제 51 조 (전산 시설 보호)

환경적, 자연적 위협으로부터 건물 및 시설을 보호하기 위해 방재, 방화, 항온·항습, 케이블 보호, 랙 실장도 관리, 비상전원 설비 등을 갖추어 최적의 상태를 유지하여야 하고 한다.

### 제 52 조 (사무실 보호 대책)

1. 사무실 보안관리 현황을 주기적으로 점검하며, 비밀 정보는 반드시 시건 장치가 되어 있는 장소에 보관한다.
2. 프린터, 팩스, 복사기의 사용 시 산출되는 문서는 즉시 회수함으로써 출력물을 타인이 가져가게 하거나, 프린터 주위에 출력물이 방치되지 않도록 하여야 한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	19 / 24

3. 방치된 노트북, 서류 등이 존재하지 않도록 클린데스크 정책을 운영하고 상시 관리하여야 한다.

## 제 10 장. 개발보안

### 제 53 조 (적용 범위)

회사에서 임직원 및 외부업체를 통해 개발한 서비스 제공 목적의 응용프로그램 및 이를 관리하고 운영하는 임직원 및 외부인력의 정보보호 활동을 대상으로 한다.

### 제 54 조 (개발보안 관리 업무의 운영)

정보보안담당자는 소프트웨어 개발 생명 주기에 고려되어야 하는 단계별 보안 활동들을 정의하여 안전한 소프트웨어 개발이 되도록 한다.

### 제 55 조 (외주개발 계약)


정보처리 시스템 담당자는 시스템 개발을 외부에 위탁하고자 하는 경우 분석, 설계, 구현, 이관 및 운영까지의 준수해야 할 보안요구사항을 계약서에 명시하여야 한다.

### 제 56 조 (외주개발 관리 및 검수)

1. 정보보호 관리자는 외부 개발업체에 대해 분석-설계-구현-시험 각 단계별로 보안요구사항 준수여부를 확인하고, 미 이행 시 개선을 요구하여야 한다.
2. 정보보호 관리자는 외부업체가 개발완료 후 보안요구사항 반영여부, 보안취약점 존재여부, 개발자 계정 및 권한 삭제 여부 등을 확인한 후 검수 또는 인수하여야 한다.
3. 또한, 정보보호 담당자는 외부인력 보안 점검을 통해 특이사항이 없을 경우 외부인력의 철수를 이행한다.

### 제 57 조 (소프트웨어 개발보안)

소프트웨어 개발보안의 상세 준수 사항은 행정안전부 및 KISA 에서 발간하는 '소프트웨어 개발보안 가이드'에 내용을 충족하도록 권고한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	20 / 24

## 제 11 장. 위험평가

### 제 58 조 (위험관리)

1. 정보보호 담당자는 정보자산의 취약·위협을 식별하고 발생빈도를 분석하여 위험을 도출하고, 이에 따른 효과적인 보호대책 수립을 위해서 위험분석 및 평가를 수행하여야 한다.
2. 위험분석 및 평가를 위해, 필요 시 외부 전문가의 지원을 받을 수 있다.
3. 위험분석 및 평가로부터 도출된 위험에 대해서는 보호대책을 수립하여 적용함으로써 위험을 관리하여야 한다.

### 제 59 조 (위험평가 업무의 운영)

위험평가 업무의 운영과 관련된 세부사항은 '위험평가 지침'을 따른다.

## 제 12 장. 보안사고 대응

### 제 60 조 (보안사고의 예방 및 대응)

1. 회사는 보안사고를 사전에 예방하고 대응할 수 있도록 통제 대책을 수립하고 적용하여야 한다.
2. 보안사고를 인지한 임직원은 정보보호 담당자에게 즉시 신고하여야 하며 보안사고 발생 시 사고 대응을 위한 조직을 구성하여 대응책을 적용하여야 한다.
3. 보안사고의 예방 및 대응에 관한 세부 사항은 '보안사고 대응 지침'을 따른다.

## 제 13 장. 보안 점검 및 감사

### 제 61 조 (보안 점검 및 감사 준수 관리)

1. 정보보호 규정 및 유관 법령에서 정하는 항목의 준수 여부를 확인하기 위하여 아래와 같은 영역에 대해 보안 점검 및 감사를 수행한다.
  - (1) 정보보호 규정의 준수 여부
  - (2) 정보보호 관련 법률 등의 준수 여부

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	21 / 24

- (3) 정보자산에 대한 침해 위험 대응 여부
  - (4) 기타 필요하다고 판단되는 영역
2. 보안 점검 및 감사 결과에 따른 지적 사항은 즉시 해결될 수 있도록 한다.
  3. 보안 점검 및 감사의 세부적인 사항은 '보안 점검 및 감사 지침'에 따른다.

### 제 62 조 (점검 및 감사 결과의 처리)

1. 보안 점검 및 감사 결과에 따른 지적 사항은 각 부서 및 부서장 책임 하에 즉시 해결될 수 있도록 한다.
2. 차후 보안 점검 및 감사 시 기존 이행 점검 결과에 따른 조치 상황을 우선으로 검토한다.
3. 보안 점검 및 감사 결과 위반사항이 많은 부서나 개인에게는 처벌할 수 있다.


## 제 14 장. 업무 연속성

### 제 63 조 (업무 연속성 계획 수립)

1. 재해, 사고, 장애 등으로 인해 발생 가능한 피해를 최소화하고 신속한 업무 재개를 위해 위기관리 측면에서 핵심 업무에 대한 백업대책, 장애대책, 비상대응 대책 등을 포함하는 업무 연속성 계획을 수립하여야 한다.
2. 업무 연속성의 세부적인 사항은 '업무 연속성 지침'에 따른다.

### 제 64 조 (업무 연속성 계획 가동)

1. 업무 연속성 계획에 따라 위기상황 발생 시 비상대책반을 소집하고 위기상황의 발생원인, 발생범위 등 관련 정보를 수집하고 분석하여야 한다.
2. 비상대책반은 업무 영향분석에 따라 핵심업무 복구 우선순위, 업무복구 목표 정의를 기준으로 업무 연속성 계획을 가동하여 위기 상황을 대응하여야 한다.
3. 위기 상황이 종료된 후에는 대응 결과를 분석하고 그에 따른 사후관리를 하여야 한다.

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	22 / 24

## 제 65 조 (업무 연속성 사후관리)


업무 연속성 계획의 위기 관리의 실효성을 확보하기 위해 모의훈련 또는 교육을 실시하고, 업무 연속성 계획을 주기적으로 검토, 개선하여야 한다.

## 부 칙

### 1. (시행일)

본 규정의 시행일은 CISO 의 최종 검토 및 최고경영진의 승인 하에 공표 후 2023 년 09 월 01 일 부터 시행한다.

### 2. (준용)

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	23 / 24

회사의 정보보호 관리 사항은 본 규정에 따라 처리하며, 정책에 명시되지 않은 사항은 관계 법령 및 사규가 정하는 바에 준한다.

### 3. (예외 적용)

다음에 해당하는 경우에는 본 규정에서 명시한 내용이라도 CISO의 승인을 받아 예외 취급할 수 있다.

- (1) 기술 환경의 변화로 적용이 불가능할 경우
- (2) 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급할 사유가 있을 경우
- (3) 기타 재해 등 불가항력적인 상황일 경우

	정보보호	문서번호	SH-A-540
		작성부서	정보보호팀
	정보보호 규정	개정번호	1
		페이지	24 / 24

제.개정 이력			
Rev.	일자	제.개정 내용	작성부서
1	2023.09.01	정보보호규정 제정	정보보호팀