



경영기획실 정보전략팀

---

# 하림 정보보호 관리 체계

2021. 3.

1. 정보보호 관리 체계
  2. 하림 정보보호 조직도
  3. 보안대시보드 수준진단
  4. 개인정보 취급 방침
  5. 개인정보 유출 대응책
  6. 정보보안 교육 실시
-

# 1. 정보보호 관리 체계



## 가. 정보보호정책 정의 및 목적

- 하림은 정보보호를 위한 최상위 정책으로서 정보보호를 위한 정보보호 관리체계의 구축, 운영, 개선 업무를 위하여 필요한 사항을 규정하여 (주)하림 구성원 및 외부인력이 준수해야 할 정보보호 활동 범위와 기준을 제시하는데 목적이 있다.

## 나. 정책의 승인 및 공표

- 정보보호 정책 및 지침의 제정, 개정, 폐기가 필요한 경우 관련 전문가 또는 실무자가 개정안을 작성하고 승인 절차에 따라 정보보호책임자의 검토를 득한 후 (주)하림 대표이사의 승인을 받아 공표 운영중이다.

## 다. 정보보호정책 및 지침 주요 내용

구분	NO.	지침명	주요내용
정책	1	정보보호정책	정보보호 정의, 목적, 범위, 역할 등 그룹 정보보호 정책 정의
정보보안	2	보안조직운영지침	보안조직 구성, 운영방안, 역할 및 책임 등에 관한 지침
	3	정보자산분류및관리지침	정보자산 파악, 자산분류, 자산라벨링 및 위험평가 등에 관한 지침
	4	보안점검지침	정기, 불시 보안점검 등 임직원 대상 보안 수준진단에 관한 지침
인원보안	5	인원보안지침	채용 및 퇴직 시 보안, 보안서약서 징구, 보안교육 등에 관한 지침
	6	외주업체관리지침	제3자 및 아웃소싱 인원보안, 계약 시 보안성검토 등에 관한 지침
관리적	7	정보시스템운영보안관리지침	서버, 네트워크, DB 등 정보시스템 운영 시 보안사항에 관한 지침
보안	8	개발보안지침	어플리케이션 개발 시 보안성 검토, 접근권한 설정 등에 관한 지침
보안	9	계정권한보안관리지침	시스템, 그룹웨어, 외부접속 사용자 등록 및 삭제 등에 관한 지침
보안	10	침해사고대응지침	보안 침해사고 발생 시 연락, 대응 및 사후관리 등에 관한 지침
보안	11	업무연속성관리지침	업무연속성을 위한 연락, 대응 및 복구 등에 관한 지침
물리적	12	물리적보안지침	주요 보호구역 설정, 관리, 출입통제 등의 물리적 보안에 관한 지침
보안	13	자산분류 및 위험평가지침	정보자산 파악, 자산분류, 자산 라벨링 및 위험평가 등에 관한 지침
개인정보	14	개인정보관리 지침	개인정보 관리범위, 절차, 접근통제, 교육등에 관한 지침
보안	15	정보보안의날 실천수칙	정보보호의 중요성에 대한 임직원들의 의식 제고

## 2. 하림 정보보호 조직도



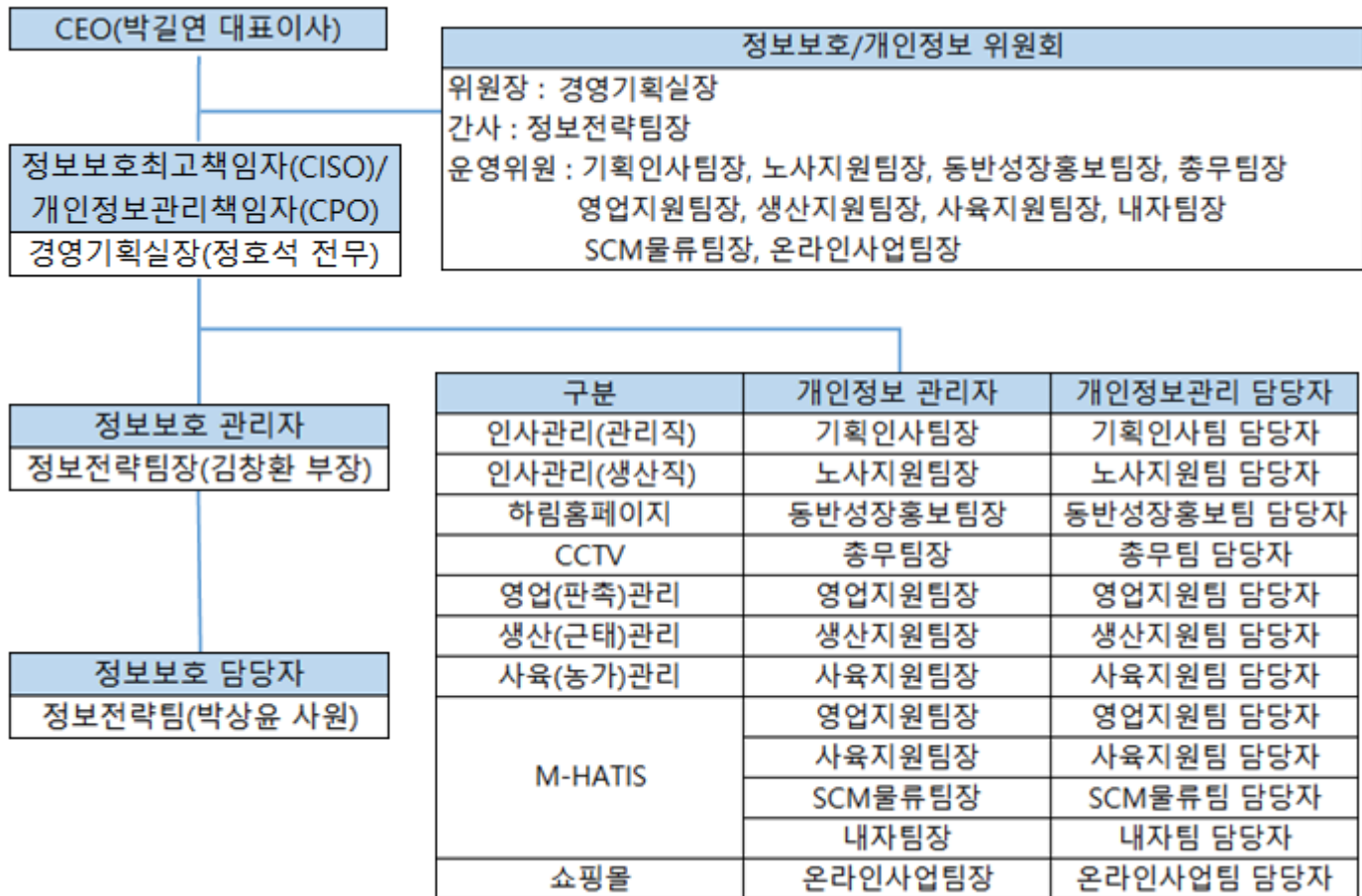
### 가. 정보 보안 조직

- 조직 내 정보보호 조직은 정보보안 업무 담당자를 지정하여 운영하며, 전문화의 원칙, 통합화의 원칙, 명령 일원화의 원칙을 준수하여 적정 인원으로 구성한다.

### 나. 정보보호 책임자의 역할

- 정보보호 총괄 및 책임
- 정보보호위원회 회의 소집 및 안건 산장
- 정보보호 관리체계 운영 관리 총괄
- 정보보호조직의 구성 및 운영
- 정보보호 정책 및 지침의 승인/승인 획득

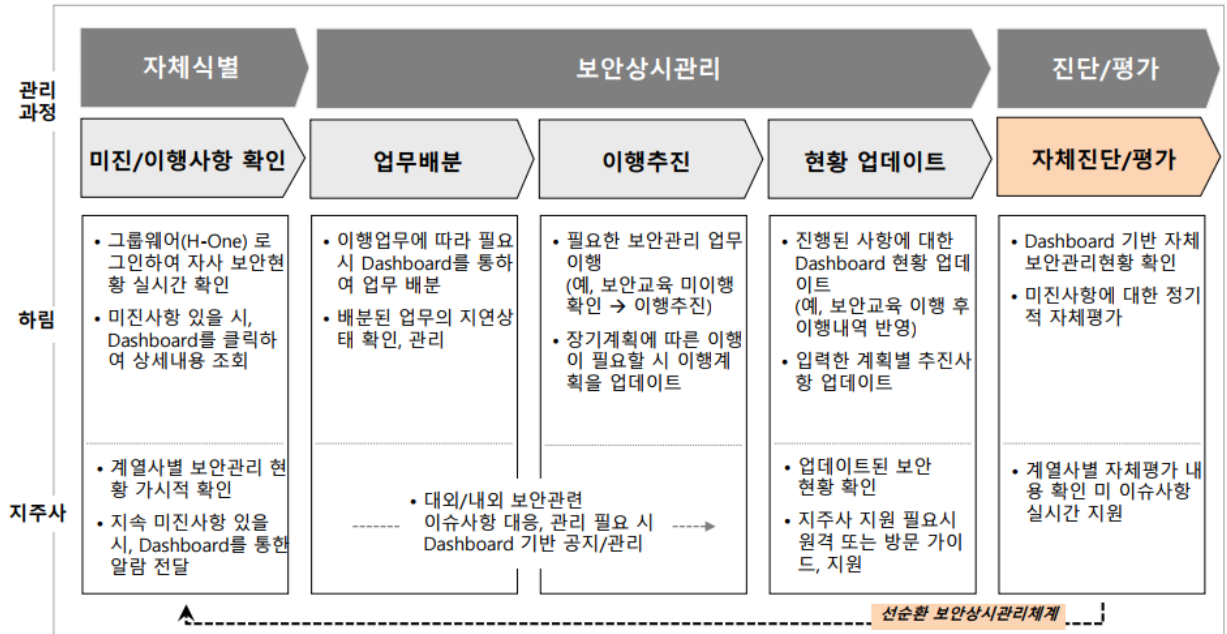
### 다. 정보보호 조직도



### 3. 보안대시보드 수준진단

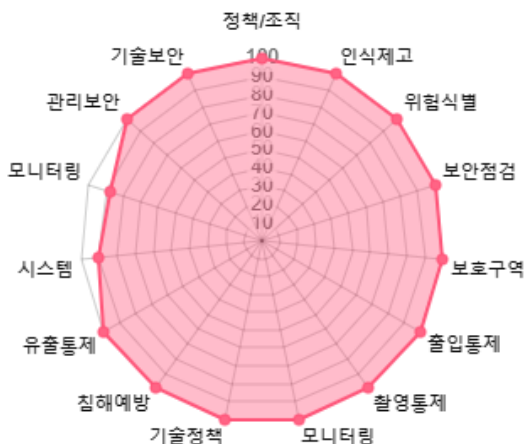
#### 가. 보안대시보드 시스템

- 하림에서 운영하는 보안대시보드 시스템을 통해 보안관리 현황 확인, 관리 및 진단을 수행하고 자체 관리 현황을 실시간 확인하는 상시 관리 체계를 운영하고 있다.



#### 나. 하림 보안대시보드 평가점수

- 하림 보안 수준은 98.0%로 하림 총괄사 평균 93.7% 보다 상위 평가 되었고 기술적 보안의 모니터링 과 시스템의 미흡항목에 대해 보완을 진행하고 있다.



관리영역	하림	총괄사 평균	전사평균
계	98.0%	93.7%	91.4%
관리적 보안	100.0%	91.7%	86.4%
물리적 보안	100.0%	96.7%	97.2%
기술적 보안	96.0%	92.3%	90.1%
개인정보 보안	100.0%	97.5%	96.9%

(2021년 진단 현황)

# 4. 개인정보 취급 방침



## 가. 하림e닭(쇼핑몰) 개인정보 취급 방침

- 하림은 쇼핑몰 가입시 수집되는 개인정보와 개인정보 수집방법 및 목적을 쇼핑몰 사용자에게 공지하고 해당 내용을 동의 받음으로써 대한민국의 개인정보 취급 관계법령 및 개인정보보호 규정, 가이드라인을 준수하고 있습니다.

### - 개인정보 수집 방법 및 목적

#### ■ 수집하는 개인정보 항목 및 수집방법

##### 가. 수집하는 개인정보의 항목

o 회사는 회원가입, 상담, 서비스 신청 등을 위해 아래와 같은 개인정보를 수집하고 있습니다.

- 회원가입시 : 이름, 생년월일, 성별, 로그인ID, 비밀번호, 자택 전화번호, 휴대전화번호, 이메일, 14세미만 가입자의 경우 법정대리인의 정보
- 서비스 신청시 : 주소, 결제 정보

o 서비스 이용 과정이나 사업 처리 과정에서 서비스이용기록, 접속로그, 쿠키, 접속 IP, 결제 기록, 불량이용 기록이 생성되어 수집될 수 있습니다.

##### 나. 수집방법

- 홈페이지, 서면양식, 게시판, 이메일, 이벤트 응모, 배송요청, 전화, 팩스, 생성 정보 수집 등을 통한 수집

#### ■ 개인정보의 수집 및 이용목적

회사는 수집한 개인정보를 다음의 목적을 위해 활용합니다.

o 서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산

콘텐츠 제공, 구매 및 요금 결제, 상품배송 또는 청구지 등 발송, 금융거래 본인 인증 및 금융 서비스

o 회원 관리

회원제 서비스 이용에 따른 본인확인, 개인 식별, 불량회원의 부정 이용 방지와 비인가 사용 방지, 가입 의사 확인, 연령확인, 만14세 미만 아동 개인정보 수집 시 법정 대리인 동의여부 확인, 불만처리 등 민원처리, 고지사항 전달

o 마케팅 및 광고에 활용

이벤트 등 광고성 정보 전달, 접속 빈도 파악 또는 회원의 서비스 이용에 대한 통계

### - 개인정보 보유기간 명시

#### ■ 개인정보의 보유 및 이용기간

원칙적으로, 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체 없이 파기합니다.

단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

가. 회사 내부방침에 의한 정보보유 사유

회원이 탈퇴한 경우에도 불량회원의 부정한 이용의 재발을 방지, 분쟁해결 및 수사기관의 요청에 따른 협조를 위하여, 이용계약 해지일로부터 00년간 회원의 정보를 보유할 수 있습니다.

나. 관련 법령에 의한 정보 보유 사유

전자상거래등에서의소비자보호에관한법률 등 관계법령의 규정에 의하여 보존할 필요가 있는 경우 회사는 아래와 같이 관계법령에서 정한 일정한 기간 동안 회원정보를 보관합니다.

o 계약 또는 청약철회 등에 관한 기록

-보존이유 : 전자상거래등에서의소비자보호에관한법률

-보존기간 : 5년

o 대금 결제 및 재화 등의 공급에 관한 기록

-보존이유 : 전자상거래등에서의소비자보호에관한법률

-보존기간 : 5년

o 소비자 불만 또는 분쟁처리에 관한 기록

-보존이유 : 전자상거래등에서의소비자보호에관한법률

-보존기간 : 3년

o 로그 기록

-보존이유 : 통신비밀보호법

-보존기간 : 3개월

## 4. 개인정보 취급 방침



### 나. 하림e닭(쇼핑몰) 개인정보 취급자

- 하림의 쇼핑몰은 개인정보 취급자를 최소화 운영하여 담당자를 제외한 인원은 개인정보에 접근할 수 없다.

X 삭제						등록
<input type="checkbox"/>	No	운영자 ID	이름	최근 접속일시	최종 비밀번호 변경일	운영자 구분
-	1	harimedak	하림e닭 대표운영자	2021-01-27 11:27	2020-09-29	대표운영자
<input type="checkbox"/>	2	cafe24customer01	카페24 CS전용	2020-08-11 11:04	2020-02-20	부운영자
<input type="checkbox"/>	3	harimedakcs	하림고객센터	2020-12-28 08:56	2020-11-10	부운영자
X 삭제						등록

### 다. 개인정보 암호화

- 쇼핑몰에서 관리되어지는 사용자의 중요 정보는 암호화 처리되어 개인정보 취급자도 열람이 불가능하다.

#### 암호화되어 저장되는 항목

- 이름, 비밀번호, 주소, 비밀번호 질문답변, 일반전화, 휴대전화, 이메일, 환불계좌 번호, 법인 번호
- 회원가입 항목 중 '사용자 추가' 항목
- 암호화 알고리즘: 가역 AES-128 / 비가역 SHA-256
- 여권 번호, 외국인 등록 번호 (외국인 등록 번호는 회원가입항목 설정에 따라 저장될 경우 AES-128로 저장됩니다.)
- 주민 등록 번호, 여권 번호, 카드 정보, 바이오 정보는 저장 항목이 없습니다.

### 라. 출처

- 하림e닭 개인정보처리 방침 페이지  
(<https://harimedak.com/member/privacy.html>)
- 하림e닭 호스팅 업체 cafe24 개인정보 암호화 관련 안내 페이지  
([https://ecsupport.cafe24.com/board/free/read.html?no=1725&board\\_no=1&category\\_no=4&cate\\_no=4&category\\_no=4&category\\_no=4](https://ecsupport.cafe24.com/board/free/read.html?no=1725&board_no=1&category_no=4&cate_no=4&category_no=4&category_no=4))

# 5. 개인정보 유출 대응책



## 가. 책임보험 가입

- 하림의 쇼핑물은 개인정보 유출 사고와 관련하여 배상체계 운영을 위한 개인정보 배상 보험에 가입되어 있어 개인정보 유출 발생시 보험을 통한 대응 체계를 갖추고 있다

- KB 손해보험 개인정보 배상 보험 증권

### 일반보험 증권

상호명 개인정보보호배상책임보험(ID) (14169) 일보  
증권번호 2020-6643749 (000) [ 1/2 페이지 ]

● 기본사항

보험기간	2020년 12월 31일 24:00 부터 2021년 12월 31일 24:00 까지 (365일간)			청약일	2020년 11월 30일
계약자	성명/성호	(주)하림	주원/사업자번호	403-81-41113	
대표이사	성명/성호	(주)하림	주원/사업자번호	403-81-41113	
대리보험자	성명/성호	(주)하림	주원/사업자번호	403-81-41113	

● 보험대상

보험대상	보험대상	보험대상	보험대상	보험대상	보험대상
보험대상	보험대상	보험대상	보험대상	보험대상	보험대상
보험대상	보험대상	보험대상	보험대상	보험대상	보험대상
보험대상	보험대상	보험대상	보험대상	보험대상	보험대상

● 목적물 (1)

목적물 소재지	(999-99) 전국일관
목적물 구분	개인정보배상-정보통신망법 의무보험
가입물건	속산입
약관사항	개인정보보호배상책임보험(B) 보통약관
납입금으로 보험자의 추가약관	소급달보 일자
재보험한 보험자의 특별약관	소급달보 일자 적용내용
비보험한 면적 추가약관	보험금 지급액

보험/특약	회계	보험금	보험금	보험금	보험금
1	개인정보보호배상책임보험(B) 보통약관	1인당	1인당	총보상한도액	사고일
	WON	200,000,000	200,000,000	200,000,000	1,000,000

※ 하림의 위조방지용 KB마크가 있는 경우에만 원본으로 인정됩니다.

발급일 2020년 12월 11일

주식회사 KB손해보험  
대표이사 양종희

### 일반보험 증권

상호명 개인정보보호배상책임보험(ID) (14169) 일보  
증권번호 2020-6643749 (000) [ 2/2 페이지 ]

● 본담정보

본담회사	납입종류	본담금	본담회사	납입종류	본담금	본담회사	납입종류	본담금
1	2020-12-31	100,000,000 (WON)	1,088,500					

● 추가상세

목적물부호	추가 상세 사항
1	소급달보일자 적용내용 : 본담, 담보 및 보험조건이 변경된 경우 변경된 조건은 해당 변경일일 24:00 부터 적용됨.

● 보험금수령 (권리사 : KB)

KB	KB	KB	KB	KB	KB
100,000					

※ 하림의 위조방지용 KB마크가 있는 경우에만 원본으로 인정됩니다.

발급일 2020년 12월 11일

주식회사 KB손해보험  
대표이사 양종희



# 5. 개인정보 유출 대응책

## - 유출 발생시 보상 내용

### 위기관리실행비용 특별약관

#### 제1조(보상하는 손해)

- ① 회사는 보험기간 중에 최초로 생긴 위기에 대하여 해당 위기에 기인해 피보험자가 부담하는 위기관리실행 비용에 대하여 보험금을 지급합니다. 단, 해당 위기가 다음에 기재된 각 호 중 하나에 해당될 경우에 한합니다.
  1. 피보험자가 공적 기관에 대하여서 문서에 의해 신고 또는 보고하는 것
  2. 신문, 잡지, 텔레비전, 라디오, 인터넷 그 외 유사한 매체에 의해 보도되는 것
- ② 회사는 위기관리실행비용에 대하여 보통약관 제4조(보상하지 않는 손해)의 규정을 적용하지 않는 것으로 합니다.

③ 위법·부당한 방법으로 인해 피해를 입게 된 고객 분을 위해 적절한 보상 및 처리가 이루어지도록 민원사항에 대한 안내 및 상담, 처리, 그리고 결과 및 통지 등 민원처리 관련 일체의 업무를 수행할 소관부서를 그룹사마다 두었습니다. 그리고 소관부서 외 금융감독원 분쟁조정제도를 통하여 구제받으실 수 있도록 하였습니다.

#### 제3조(보상하는 손해)

회사는 대한민국 내에서 피보험자의 업무수행 과정이나 그러한 목적으로 소유, 사용, 관리하는 "개인정보"의 우연한 유출·분실·도난·위조 또는 훼손(이하 「사고」라고 합니다)으로 인하여, 피보험자가 개인정보주체에게 법률상 손해배상책임을 부담함으로써 입은 손해(이하 「손해」라고 합니다)를 보상하여 드립니다.

1. 피보험자가 피해자에게 지급할 책임을 지는 법률상의 손해배상금
2. 계약자 또는 피보험자가 지출한 아래의 비용
  - 가. 피보험자가 제11조(손해방지의무)제1항 제1호의 손해의 방지 또는 경감을 위하여 지출한 필요 또는 유익하였던 비용.
  - 나. 피보험자가 제11조(손해방지의무)제1항 제2호의 제3자로부터 손해의 배상을 받을 수 있는 그 권리를 지키거나 행사하기 위하여 지출한 필요 또는 유익하였던 비용
  - 다. 피보험자가 지급한 소송비용, 변호사비용, 중재, 화해 또는 조정에 관한 비용
  - 라. 보험증권상의 보상한도액내의 금액에 대한 공탁보증보험료. 그러나 회사는 그러한 보증을 제공할 책임은 부담하지 않습니다.
  - 마. 피보험자가 제12조(손해배상청구에 대한 회사의 해결)제2항 및 제3항의 회사의 요구에 따르기 위하여 지출한 비용

#### 【설명】

제3자로부터 손해의 배상을 받을 수 있는 경우에 피보험자가 손해배상청구를 위해 내용증명, 재산조사, 강제집행 등을 수행하고자 지출한 각종 비용을 의미합니다.

#### 제1조(보상하는 손해)

- ① 회사는 보험기간 중에 최초로 생긴 위기에 대하여 해당 위기에 기인해 피보험자가 부담하는 위기관리컨설팅 비용에 대하여 보험금을 지급합니다.
- ② 회사는 위기관리컨설팅비용에 대하여 보통약관 제4조(보상하지 않는 손해)의 규정을 적용하지 않는 것으로 합니다.

# 5. 개인정보 유출 대응책

## 나. 보안 인증

- 하림의 쇼핑몰 호스팅 업체 Cafe24와 KT 데이터센터는 정보통신망의 안정성, 신뢰성 확보를 위한 관리적, 기술적, 물리적 보호조치에 관한 기준을 통과한 ISMS 인증서를 보유하고 있으며 주기적으로 갱신 되어지고 있습니다.

항목	내용 증명
Cafe24 ISMS 인증서	 <p>정보보호 관리체계 인증서</p> <p>인증번호 : ISMS-KISA-2021-008</p> <p>발행처 : 카페24 주식회사</p> <p>대표자 : 이재석</p> <p>인증의 범위 : 쇼핑몰호스팅, 웹호스팅 서비스 운영</p> <p>유효기간 : 2021.01.20 ~ 2024.01.19</p> <p>「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.</p> <p>2021년 01월 20일</p> <p>ISMS 한국인터넷진흥원장</p>
KT ISMS 인증서	 <p>정보보호 관리체계 인증서</p> <p>인증번호 : ISMS-KISA-2019-042</p> <p>발행처 : KT데이터</p> <p>대표자 : 황광규</p> <p>인증의 범위 : KT IDC 및 비즈니스부품(비즈에어, 초포장, CDN 등), KT Cloud 인프라 운영</p> <p>유효기간 : 2019.11.27 ~ 2022.11.26</p> <p>심사수령기관 : 한국인터넷진흥원</p> <p>「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.</p> <p>2019년 11월 27일</p> <p>ISMS 한국인터넷진흥원장</p>

# 6. 정보보안 교육 실시

## 가. 정보보안 교육

- 하림은 관리직군을 대상으로 올원에듀를 통한 인터넷 강의로 개인정보 보호 교육을 매년 실시 하고 있습니다.

번	교육시작일	교육종료	소속	이름	과목명	진도	최종평	총	수료여
1	2020-05-18	2020-06-05	주식회사 하림(본사신선)	강기철	개인정보보호교육-1	100			수료
2	2020-05-18	2020-06-05	주식회사 하림(본사신선)	강병권	개인정보보호교육-1	100			수료
3	2020-05-18	2020-06-05	주식회사 하림(본사신선)	강상우	개인정보보호교육-1	100			수료
636	2020-05-18	2020-06-05	주식회사 하림(본사신선)	황재연	개인정보보호교육-1	100			수료
637	2020-05-18	2020-06-05	주식회사 하림(본사신선)	황종기	개인정보보호교육-1	100			수료
<p>수료 : 637명 미수료 : 0명</p> <p>위 사람은 상기 교육과정을 이수하였음을 확인합니다. 2020년 06월 25일</p> <p>교육훈련기관 주식회사 올원에듀</p>									

## 나. 정보보안 교육

- 하림e샵(쇼핑몰)의 주기적인 보안 점검 하고 있으며, 관리부서인 온라인사업팀에 대해 취약점에 대한 보안조치를 하도록 가이드하고 있습니다.

문서번호 : 정보전략팀 제 21-0318-195호

시행일 : 2021-03-18 (보관연한: 3년)

수신 :

참조 : 참조처 참조

제목 : 하림e샵(쇼핑몰) 웹 취약점 진단 결과 보고의 건.

기안	팀장	실장	사장
박상윤	김장환	정호석	윤석훈
2021-03-17 10:15:32	2021-03-17 11:23:49	2021-03-17 14:59:47	2021-03-18 08:49:05

하림e샵(쇼핑몰)의 안정적인 서비스와 보안 강화 및 사전 Risk 예방을 위한 취약점 진단 결과를 아래와 같이 보고드립니다.

-      아      래      -

**1. 목      적**  
가. 하림e샵 쇼핑몰의 안정적이고 최적화된 서비스 제공  
나. 공개된 하림e샵의 웹 취약점에 대한 사전 예방 및 확인

**2. 취약점 진단 개요**  
가. 진단일자 : 2021. 03. 11  
나. 진단방법  
1) 웹 서버 취약점 점검 정책에 의거하여 점검 진단  
2) OWASP(The Open Web Application Security Project) 정책에 의거하여 웹 취약점 점검 진단  
다. 진단대상 : 하림e샵(쇼핑몰) [www.harimedak.com](http://www.harimedak.com)

**3. 취약점 진단 결과**  
가. 웹 서버 취약점 점검 정책에 의거하여 진단 결과: 총 850개의 점검 항목 중 827개 안전 23개 취약

총점검개수	1-정보	2-낮음	3-보통	4-높음	5-위험	합계
850	17	2	4	0	0	23

분류	점검항목수	1-정보	2-낮음	3-보통	4-높음	5-위험	합계
웹 어플리케이션 취약점	237	3	2	0	0	0	5
취약한접근통제	46	1	0	0	0	0	1
입력값검증부재	143	0	0	0	0	0	0
부적절한 환경 설정	56	7	0	3	0	0	10
부적절한 에러 처리	15	0	0	0	0	0	0
부적절한 데이터 관리	37	5	0	0	0	0	5