정보보호를 위한 활동

매일유업은 정보보호 관리체계의 지속적인 고도화를 통해 정보자산 및 개인정보를 체계적으로 보호하고 있습니다. 2025년에는 ISMS 요구 수준에 부합하도록 관리체계를 정비하고 주요 정보 시스템과 IT 자산을 대상으로 정기 점검과 상시 모니터링을 수행함으로써 정보보안 사고 예방 활동을 강화하였습니다.

2025년 정보보호 주요 활동

2025년 주요 활동	수행 시기 (월)	상세 활동 내역
PC OS 업그레이드	1~2월	기술지원 종료로 보안에 취약한 임직원 PC OS_WIN10 버전을 WIN11 전환
모의 해킹(주요시스템)	3-4월	내부 업무 서비스 취약점 가시성 확보 및 조치
방화벽 및 사업장 네트워크 장비/ 펌웨어 업데이트	5~6월	네트워크 장비 200 여대 보안 취약점 펌웨어 업데이트 진행
정보보호 관리체계 정비	6월	관리대상을 16개 항목으로 구분하고 ISMS (Information Security Management System) 요구 관리 수준으로 보안 지침 업데이트
전사 IT자산 대장 실사	7월	서버, PC, 노트북 뿐만 아니라 네트워크 장비, 소프트웨어 라이선스, 클라우드 리소스, 그리고 그 안의 '개인정보_데이터'까지 식별
인터넷 접점 자산 식별	8월	외부 인터넷에 노출되어 있는 모든 IT 자산을 찾아내고 보안 상태를 파악
인터넷 접점 시스템 취약점 점검	9월	자산 식별 이후에 반드시 수행해야 하는 핵심 보안 단계로 식별된 인터넷 접점, 자산들이 실제로 공격자에게 뚫릴 위험이 있는지 점검
백업 복구 훈련	10월	보안 사고나 시스템 장애 발생 시 비즈니스 연속성 유지 및 대비하기 위한 실전 연습
개인정보 DB암호화 고도화	12월	개인정보 취급 시스템 대상으로 데이터 암호화 시스템 도입
인적 보안 리스크를 관리 활동 (임직원 보안 의식 내재화 강화)	정기	전 임직원 대상 개인정보보호 법정 교육 및 직무별 심화 교육 실시, '클린 데스크', '비밀번호 변경 캠페인' 등 일상 속 보안 실천 독려

※ ISMS 는 정보자산의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 보장하기 위해 관리적, 기술적, 물리적 보호조치를 통합적으로 운영하는 정보보호 관리체계를 의미함

정보보호를 위한 활동

내부보안 정책에 따라 개인정보취급 시스템 전반에 대한 정기적인 취약점 점검 및 개선활동을 수행하고 있습니다. 2025년도 시스템 보안 점검(1월)결과, 우선순위에 따라 단기.중기. 장기로 기간별 조치 계획으로 수립하고, 취약요소에 대해서는 접근통제 강화, 시스템 설정 보완, 보안 패치 적용 등 필요한 조치를 통해 위험도 수준을 완화하고 있습니다.

2025년 위험평가 및 취약점 개선활동

(2025년 12월 말 기준)

점검 대상	점검 항목 주1)	최초 점검 (1월) 취약점 식별 건수	우선 순위 결정 주2) 단기개선 건수
OS 시스템	[개인정보취급시스템 내 외부침입 차단/예방점검] ✓ 시스템 보안설정 관리 ✓ 권한, 로그, 접근 관리 ✓ 서비스,패치, 계정 관리 ✓ 파일 및 디렉터리 관리	2,982 건	2,305 건
DB 시스템		373 건	26 건
WEB 시스템		405 건	43 건
합계	14,540 건	3,760 건	2,374 건

구분	위험도 정의	단기 개선조치 목표 건수 주3)	단기 개선 조치 건수	이행 점검(9월) 취약점 개선비율
최상	비인가자가 이를 통해 시스템의 **관리자 권한을 획득**하거나 서비스를 중지시키는 등 큰 장애를 일으킬 수 있는 위험	6 건	6 건	100%
상	비인가자가 이를 통해 시스템의 **사용자 권한을 획득**하거나 서비스를 중지시키는 등 큰 장애를 일으킬 수 있는 위험	1,235 건	1,235 건	100%
중	비인가자가 복수의 **취약점을 이용하여 시스템에 접근**이 가능하거나 장애를 일으킬 수 있는 위험	690 건	690 건	100%
하	시스템에 직접적인 피해를 일으킬 수 없으나 공격에 활용할 수 있는 **시스템 정보를 획득할 수 있는 위험**	332 건	332 건	100%
최하	비인가자 혹은 인가자가 공격과 직접적인 연관은 없으나 시스템에 관한 **불필요한 정보를 획득할 수 있는 위험**	110 건	110 건	100%
	합계	2,374 건	2,374 건	100%

주1) 평가기준은 ISMP-P 인증기준 3개 영역/102개 항목 중 시스템 보안 영역이며, 위험요인인 개인정보취급시스템에 외부침입을 차단,예방조치 목적으로 점검하였음
주2) 위험처리를 위해 수립된 보호대책은 위험도를 기준으로 난이도 (실행 용이성), 비용 등의 제반 요소를 고려해 우선 조치 결정
주3) 개선조치 시기 : 단기 (100일 이내), 중기 (1년 미만), 장기 (1년 이상) 로 구분하여, 정기 이행점검 시행

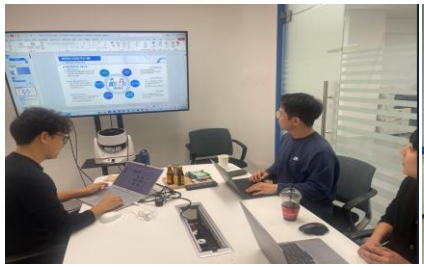
개인정보보호를 위한 활동

매일유업은 임직원 및 이해관계자를 대상으로 한 체계적인 교육과 점검을 통해 개인정보보호 이행 수준을 지속적으로 제고하고 있습니다. 전사 차원의 법정 교육을 정기적으로 실시하는 한편, 대리점 및 수탁사를 대상으로 현장 점검과 업무 특성을 반영한 맞춤형 교육을 운영함으로써 개인정보의 안전한 처리와 관리 역량 강화를 추진하고 있습니다.

2025년 개인정보보호 관리점검 및 교육

2025년 주요 활동	방법	일시	참여 인원 및 업체	주요 내용
전 임직원 대상 개인정보보호 교육	온라인 교육	3월 10일 ~ 3월 21일	1,897명	• 전사 임직원 대상 법정필수 교육 이수 • 자가진단을 통해 개인정보보 내용 점검 • 교육 내용은 개인정보보호법령과 데이터3법 이해, 개인정보 처리지침, 피해구제방안, 사고대응 사례, 인공시대의 개인정보 활용 및 정보보안 방안 제시
대리점 대상 개인정보보호 관리현황 방문 점검	현장 대면	7월 1일 ~ 8월 14일	대리점 47개소	• 협력사와의 상생협력을 위하여 현장 방문을 통한 개인정보보호 관리수준 점검 활동
수탁사 대상 개인정보보호 관리점검 및 맞춤형 교육	온라인 교육 현장 대면	11월 20일 ~ 12월 31일	고객 상담원 시스템유지보수개발자, 대리점주 등 121명	• 개인정보보호 점검 체크리스트(15개 항목)활용하여 미비사항 조치, 현장 맞춤형 교육 및 가이드 제공

현장 점검 활동 및 맞춤형 교육 사례





no	cord	대분류	중분류
1	1-1	고객 개인정보 서류 보관	가입신청 절차 준수
2	1-2		가입신청서류 관리
3	1-3		고객 개인정보 서류 관리
4	2-1	개인정보 취급 PC보안	백신 설치 및 설정
5	2-2		화면보호기 설정
6	2-3		PC 로그인 암호 설정
7	3-1	고객 개인정보 관리 및 파기	개인정보처리방침 수립 및 공개
8	3-2		개인정보 파일 보관 및 접근통제
9	3-3		외부저장매체 사용
10	3-4		P2P 사용 제한
11	3-5		개인정보처리시스템 사용 및 기술적 보호조치
12	3-6		개인정보 파기
13	4-1	물리보안	접근통제
14	4-2		CCTV 운영

No.	점검내용
1	매일유업으로 부터 제공받은 개인정보를 목적 외로 이용하거나 제3자에게 제공하지 않고 있다.
2	매일유업의 동의 없이 개인정보를 제위탁하지 않고 있다.
3	연 1회 이상 개인정보취급자에게 자체교육 또는 외부교육을 수행하고 있다.
4	개인정보에 접근하는 직원을 최소한으로 제한하여 관리하고 있다.
5	전출·사무실에 대한 출입 통제변호기, 자물쇠, 지문 등을 수행하고 있다.
6	개인정보가 포함된 출력물 또는 FAX 문서는 접근권자가 있는 캐비닛 등에 보관하고 있다.
7	개인정보가 포함된 문서파일은 PC에 보관 시, 별도의 폴더에 암호를 설정하거나 파일에 암호를 설정하여 보관하고 있다.
8	개인정보가 포함된 파일(엑셀, 이미지 등) 및 출력물은 이용목적 달성 후 복구할 수 없도록 파기하고 이를 기록 관리하고 있다.
9	개인정보취급자 PC에 악성 프로그램 등을 방지·차단하기 위한 백신 소프트웨어 등의 보안 프로그램이 설치되어 있고, 실시간 감시 기능이 동작하고 있
10	최서내 PC, 노트북에 백신 소프트웨어 등의 보안 프로그램이 최신버전을 유지하도록 자동 업데이트 기능을 사용하거나 매일 업데이트하고 있다.
11	업무용 PC 등의 단말기에서 P2P, 도박사이트와 같은 업무와 무관한 프로그램의 설치 및 웹사이트 접속을 차단하고 있다.
12	개인정보취급자의 PC에 화면보호기가 적용되어 있으며, 다시 시작할 때 로그온 화면을 표시하도록 설정되어 있다. (15분 이내)
13	윈도우 업데이트 등 운영체제 패치를 정기적으로 실시하고 있다. (XP 사용 불가)
14	휴대용 저장매체(USB, 외장하드) 반출입 관리 및 비인가 저장매체 사용을 통제하고 있다.
15	개인정보처리시스템, PC의 비밀번호를 최소 8자리, 숫자+영문+특수문자 혼합으로 설정하고 있다.