S.26 개인정보처리시스템 보호조치 가이드

목차

1. 목적

개인정보처리시스템이 법적 요구사항을 충족하고 안전하게 운영될 수 있도록 적용해야 하는 보호조치 사항을 정의합니다.

2. 적용 범위

개인정보를 다루는 어드민의 경우 법적 요구사항을 충족하기 위하여 이 가이드에 따라 보호조치를 적용해야 합니다.

3. 정의

1) "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말합니다.

2) "개인정보취급자"란 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기,연동 등의 업무를 하는 자를 말합니다.

3) "망분리"라 함은 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 말합니다.

4) "접속기록"이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말합니다.

5) "어드민"이란 특정 서비스의 관리를 목적으로 해당 서비스에 수반되는 일련의 유지보수, 데이터 갱신, 서비스 운영 등의 작업을 위한 웹 페이지 또는 도구를 말합니다.

6) "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템(예: 개인정보를 취급하는 DB 또는 Admin 시스템 등)을 말합니다. 어드민에서 개인정보를 처리하는 경우 개인정보처리시스템으로 분류하고 개인정보 DB 를 이용한 개인정보처리시스템 구축 시 사전에 개인정보 ____) 및 정보보호 담당부서(_____)에 내용을 공유합니다.

4. 개인정보처리시스템 보호조치

4.1 담당자 지정

1) 개인정보처리시스템 설치, 운영, 종료까지 관리할 담당자를 지정하여야 합니다.
2) 담당자는 개인정보취급자로 분류되어 정기적으로 개인정보교육을 이수하여야 합니다.

4.2 서버 구성

1) 개인정보처리시스템은 독립된 서버에 구성하여야 합니다.
2) 서비스가 운영중인 서버 또는 개인 PC 등에 개인정보처리시스템을 구성하지 않아야 합니다.
3) 개인정보처리시스템은 데이터베이스와 분류하여 구성하여야 합니다.

4.3 IP 할당

1) 개인정보처리시스템은 외부에서 접근할 수 없도록 반드시 사설 IP 를 할당해야 합니다.
2) VIP, 공인 IP 등을 할당받거나 Proxy Server 등을 경유하여 외부에서 접근하지 않아야 합니다.
3) 외부에서 접근이 필요한 기능은 해당 메뉴를 분리하여 별도의 서버에 구축하여야 합니다.
4) 부득이하게 외부의 접근이 필요한 경우 가급적 SSLVPN 을 통해 접근하도록 합니다.

4.4 도메인 등록

1) 개인정보를 포함하고 있는 실 서비스 DB 를 연동하는 개인정보처리시스템은 외부에서 DNS 쿼리 시 정보가 노출되지 않도록 사내 도메인을 사용해야 합니다.

-
  - 개인정보처리시스템 전용 도메인 : _____
  - 도메인 신청 : _____

2) 외부에서 직접 접근이 필요한 파트너 어드민의 경우 서비스 도메인을 사용해야 합니다.

4.5 인증

1) 개인정보처리시스템의 인증은 업무용 계정을 사용하여 접속할 수 있도록 구현하여 퇴사 등 인사 정보가 반영되도록 해야 합니다.

-
  - 업무용 계정 로그인 : _____
  - HelloMIS 문의 : _____
  - CAS 또는 inhouse-SSO 를 개인정보처리시스템의 인증 API 로 사용하는 것은 지양

2) 1 인 1 계정 사용을 원칙으로 합니다.
3) 비밀번호는 복잡도 설정(영문, 숫자, 특수문자 포함 8 자리 이상) 및 변경주기(3 개월)를 따라 안전하게 적용해야 합니다.
4) 개인정보처리시스템이 다루는 개인정보의 중요도에 따라 2 차 인증(카카오톡 OTP)을 적용할 수 있습니다.

-

- OTP 연동 문의 : _____

5) 일정 시간(최대 120 분) 동안 입력이 없는 경우 로그인 세션 해제하여 비인가 접근에 대해 보호해야 합니다.

4.6 접근 권한

1) 사용자의 업무 목적에 맞게 접근 권한을 최소화하고 접근 권한을 차등 부여해야 합니다.
2) 개인정보처리시스템에 장기간(최대 30 일) 미접속 시 접근 권한을 회수하고 신규 요청을 통해 새롭게 할당해야 합니다.
3) 인사이동으로 인한 조직 변경 시 권한을 회수하고 신규 요청을 통해 새롭게 할당해야 합니다
4) 로그인 인증 시 5 회 이상 실패하는 경우 계정을 잠그거나 일정 시간(30 분 이상) 로그인 제한합니다.

4.7 암호화

1) 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 합니다.
2) 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등 고유식별정보 및 지문, 홍채, 음성, 필적 등 바이오정보는 안전한 암호알고리즘으로 암호화하여 저장하여야 합니다.
3) 비밀번호, 고유식별번호 등 개인정보를 전송하는 경우 SSL/TLS 등의 암호화 방식을 적용하여야 합니다.
4) HTTPS 적용 시 부분 암호화가 아닌 개인정보처리시스템 전체 적용하도록 합니다.
5) 인증서는 유효기간 전 반드시 갱신하여야 합니다.

-
  - 인증서 요청 : _____
  - 인증서 다운로드 : **----------**(권한필요)

4.8 망분리 메뉴 적용

1) 개인정보처리시스템에서 개인정보처리시스템의 권한부여(권한 생성,수정,삭제), 개인정보를 다운로드 또는 파기할 수 있는 경우 물리적 또는 논리적으로 망분리 하여야 합니다.
2) 망분리가 필요한 경우 일반 메뉴에서 분리하여 외부 및 사내 IP 에서의 접근을 차단하고 VDI 대역에서만 접근할 수 있도록 조치해야 합니다.

3) 망분리 메뉴 적용 시 해당 메뉴는 취급자용 VDI 방화벽의 통제를 받아 미승인 접근에 대해서는 모두 차단됩니다.

- 해당 서버 외에 다른 서버 또는 외부에서 컨텐츠를 가져오는 경우는 접근이 차단될 수 있습니다.
- 어드민과 동일한 서버에 컨텐츠를 구성하거나 보안정책 신청 시 함께 신청해야 합니다.

4.9 개인정보 마스킹

1) 개인정보 업무처리를 목적으로 개인정보를 조회, 출력하는 경우 마스킹을 통해 노출을 최소화할 수 있습니다.
2) 그 외 개인정보 마스킹에 대한 세부사항은 정보보호 활동규칙 S.05 정보 출력 마스킹 가이드를 따른다.

4.10 개인정보 관련 로그 연동

1) 개인정보처리시스템에 대한 접근권한 부여 기록, 퇴직 등 인사이동의 발생에 따른 변경 또는 말소에 대한 내역을 기록하여야 합니다.
2) 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 기록하여야 합니다.
3) 권한 부여, 변경, 말소 및 접속기록에 대해 개인정보처리시스템에 로그를 별도로 생성하고 전사 보안 로그 장비에 연동하여야 합니다.
4) 아래 양식의 로그를 생성하여 해당 웹서버 별도의 경로에 저장하여야 합니다.

구분	설명	
로그 형식	time(시간), user(사용자_id or 사용자_email), ip(사용자가 접속한 단말의 IP 정보), action(개인정보 조회, 개인정보 다운로드/파기, 사용자 권한부여/수정/삭제), menu(어드민 메뉴명), vdi(망분리 여부), url(요청 URL), param(요청 파라미터)	
필드 설명	time	어드민에서 해당 액션이 실행된 시간을 기록
	user	로그인 기반으로 로그인 시 사용된 계정을 기록 ID or email 등 형식에 구애받지 않고, 사용자 식별을 위한 식별자를 기록
	ip	어드민에 접속한 단말기의 IP 정보를 기록
	action	어드민 로그인 시 : user_login 어드민 로그아웃 시 : user_logout 개인정보 조회 시 : privacy_view 개인정보 다운로드 시 : privacy_download 개인정보 파기/삭제 시 : privacy_delete 사용자 권한 부여 시 : user_add 사용자 권한 수정 시 : user_edit 사용자 권한 삭제 시 : user_delete
	menu	사용자가 접근한 메뉴 이름

	vdi	vdi 의 값은 해당 메뉴가 취급자용 VDI 에서 접근해야 하는 경우 vdi=o, 그 외 일반 PC 에서 접근해야 하는 vdi=x 로 표기 망분리 메뉴에 대해서는 개인정보보호셀에서 어드민 메뉴 분석 후 공유
	url	요청 URL
	param	요청 파라미터에는 해당 액션에 대한 상세 내용이 기록되어야 함. 개인정보 조회/다운로드/수정/삭제 시 어떠한 사용자의 정보를 조회/다운로드/수정/삭제 했는지. (로그 예시) time=2015-01-01 21:25:44, user=admin.kakao, ip=10.41.132.1, action=privacy_download, menu=exceldown, vdi=o, url=https://admin.sample.kakao.com/sms/download, param={index:kakao,} 사용자 권한 부여/수정/삭제 시 어떠한 사용자를 어떤 권한으로 부여했는지, 수정했는지, 삭제했는지 (로그 예시) time=2015-01-01 21:25:44, user=admin.kakao, ip=10.41.132.1, action=user_add, menu=adduser, vdi=o, url=https://admin.sample.kakao.com/sms/search, param={user:user.kakao, role:admin, status:A} 단, 기록되는 로그에는 개인정보가 포함되지 않아야 함.

5) 저장된 로그 경로에 대해 정보보호팀()에 공유해야 합니다.

생성된 로그에 대해 인프라보안셀에서 스플렁크 데몬을 설치하여 로그를 연동합니다. 따라서, 로그 연동 시 운영툴 서버에 아래와 같이 splunkforwarder 데몬이 설치/구동됩니다.

6) 어드민 접속 로그는 2 년 이상 보관, 어드민 권한 부여 로그는 5 년간 보관해야 합니다.

4.11 보안 검수

개인정보처리시스템 구축 완료 후 정보보호팀(@@security)에 취약성 점검을 요청해야 합니다.

5. 예외 적용

1. 본 가이드에 정의 되지 않은 용어에 대해서는 개별 규정에 정의된 용어의 기준을 따른다. 다만, 용어 정의가 되어 있지 않은 경우는 법률 및 전문용어집을 인용할 수 있다.
2. 다음 각 호에 해당하는 경우에는 개인정보보호책임자의 승인을 통해 예외를 적용할 수 있다.
   a. 기술환경의 변화로 적용이 불가능한 경우
   b. 기술적・관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있는 경우
   c. 기타 재해 등 불가항력적인 상황인 경우

부칙 <2018.11.26>

제 1 조(시행일) 본 규정은 2018 년 11 월 26 일로부터 시행한다.