사용자 단말기 보안관리 지침

제정 2019. 3. 7.
개정 2022. 7. 1.

제1조(목적) 이 지침은 「교육부 정보보안기본지침」제72조, 「부산대학교 정보보안기본지침」제67조, 「개인정보보호법」 제29조, 「개인정보보호법시행령」 제30조에 따라 부산대학교(이하 “학교”라 한다) 내에서 학교 정보통신망을 이용하는 사용자 단말기(PC 등)의 보안준수 세부 기준을 정하여 사용자 단말기의 보안을 강화하는 데 있다.

제2조(용어 정의) 본 지침에서 사용하는 용어의 정의는 다음과 같다.

① “정보보안”이란 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 말한다.

② “사용자”란 소속기관의 장으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 자를 말한다.

③ “정보통신망”이란 「전기통신기본법」 제2조제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신하는 정보통신체제를 말하며 정보시스템 일체를 포함한다.

④ “단말기”란 PC·노트북 등을 말하며, 스마트폰은 제외한다.

⑤ “보안관리 소프트웨어”란 단말기 보안 소프트웨어로서 패치관리시스템(PMS: 백신, 보안패치관리, 내PC지키미), 개인정보파일 진단 프로그램이 사용자단말기에 설치하는 보안관리 소프트웨어를 말한다.

제3조(적용 범위) 학교 내에서 정보통신망을 이용하는 전체 단말기를 대상으로 한다.

제4조(보안준수사항) 학교 내에서 사용하는 모든 단말기를 대상으로 다음 각 호에 대한 보안대책을 사용자에게 지원하며, 사용자는 이를 반드시 준수하여야 한다.

1. 학교에서 제공하는 보안관리 소프트웨어(①. PMS, ②. 개인정보파일진단 프로그램)를 반드시 설치·실행하여 단말기를 사용하여야 한다.

【단말기 보안관리 소프트웨어 리스트】

단말기 보안관리 소프트웨어		기능
1 패치관리시스템 (PMS)	백신	바이러스 치료 소프트웨어
	내PC지키미	사용자 보안 진단 소프트웨어
	자동보안패치	운영체제 및 응용프로그램 보안 패치
2 개인정보파일 진단 프로그램		개인정보파일 진단 소프트웨어

제5조(사용자 지원) ① 정보화본부장은 사용자가 캠퍼스내에서 학교 통신망에 단말기(PC 등)로 접속할 경우 보안관리소프트웨어를 자동 설치·실행하는 시스템을 도입하여 사용자를 지원할 수 있다.

② 정보화본부는 사용자에 대한 PC보안강화 및 자산조사를 위한 목적으로만 단말기의 IP, OS, HW규격정보(CPU type, 메모리용량, 디스크용량) 등을 자동 수집할 수 있다.

③ 정보화본부는 1항에도 불구하고 「개인정보보호법」에 따라 개인정보수집은 하지 말아야 하며, 단말기내에 개인정보 수집은 불가능하도록 조치를 취해야 한다.

제6조(이용 제한) 정보화본부장은 학교 내에서 보안관리소프트웨어를 설치하지 않은 단말기는 학교 정보통신망 사용을 제한할 수 있다.

부 칙

이 지침은 행정업무용 단말기에 대해서 2019년 3월 7일부터 시행한다.

부 칙

이 지침은 행정업무용 단말기에 대해서 2022년 7월 1일부터 시행한다.