’23.7.6. 개정고시(안)	’23.9.22. 최종 고시결과
제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제29조와 같은 법 시행령(이하 "영"이라 한다) 제16조제2항, 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.	**제1조(목적)** 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제29조와 같은 법 시행령(이하 "영"이라 한다) 제16조제2항, 제30조 **및 제30조의2**에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.
제2조(정의) 1.~14. 동일 **15. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 접속하는 단말기를 말한다.**	**제2조(정의)** 1.~14. 동일 **<삭제>**
제5조(접근권한의 관리) ① 개인정보처리자는 개인정보처리시스템에---------- ③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 **전자적으로** 기록하고, 그 기록을 최소 3년간 보관하여야 한다.	**제5조(접근권한의 관리)** ① 개인정보처리자는 개인정보처리시스템에---------- ③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 **<삭제>** 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
제6조(접근통제) ② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 안전한 인증수단을 적용하여야 한다.	**제6조(접근통제)** ② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 **인증서, 보안토큰, 일회용 비밀번호 등** 안전한 인증수단을 적용하여야 한다. **다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.**

제7조(개인정보의 암호화) ④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다. **다만, 고유식별정보, 생체인식정보를 정보통신망(내부망을 포함한다)을 통하여 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야한다.** ⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 **상용 암호화 소프트웨어 또는** 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.	**제7조(개인정보의 암호화)** ④ ---------- ---------- ---------- **<삭제>** ⑤ ---------- ---------- ---------- **<삭제>** 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.
제8조(접속기록의 보관 및 점검) **① 개인정보처리자는 개인정보처리시스템에 접속한 자에 대한 접속기록을 생성하고 3개월 이상 보관·관리하여야 한다.** ② 제1항에도 불구하고 개인정보처리자는 개인정보취급자의 접속기록은 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다. **③ 제1항 및 제2항에 따른 접속기록은 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무를 포함하여야 한다.** ⑤ 개인정보처리자는 **제1항 및 제2항에 따른** 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.	**제8조(접속기록의 보관 및 점검)** **<삭제>** **① 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 1 년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.** **③ <삭제>** ⑤ 개인정보처리자는 **<삭제>** 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

제10조(관리용 단말기의 안전조치) **개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.** **1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치** **2. 본래 목적 외로 사용되지 않도록 조치** **3. 악성프로그램 감염 방지 등을 위한 보안조치 적용**	**제10조(관리용 단말기의 안전조치)** **<삭제>**
제11조(물리적 안전조치) ③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.	**제10조(물리적 안전조치)** ③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. **다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.**
제13조(출력·복사시 안전조치) ① ---------- ② ---------- **③ 개인정보처리자가 업무의 특성으로 인해 민감정보 또는 고유식별정보가 포함된 개인정보를 불가피하게 인쇄해야 하는 경우로서 다음 각 호의 어느 하나에 해당하는 때에는 내부 관리계획으로 정하는 바에 따라 인쇄자, 인쇄일시 등을 기록하는 등 종이 인쇄물의 안전한 관리를 위해 필요한 조치를 하여야 한다.** **1. 공공기관이 민감정보 또는 고유식별정보를 개인정보파일에 포함하여 관리하는 경우** **2. 개인정보처리자가 5만명 이상의 정보주체에 관하여 민감정보를 처리하고 있는 경우** **④ 제3항에 따른 종이 인쇄물에 대하여는 파기하는 절차, 파기 여부의 확인 등을 포함하는 파기계획을 수립하고 주기적으로 점검하는 등 필요한 조치를 하여야 한다.**	**제12조(출력·복사시 안전조치)** ① ---------- ② ---------- **③, ④ 삭제**