제7조 개인정보의 암호화

제7조(개인정보의 암호화)

❶ 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

❷ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

❸ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

❹ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과

❺ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

❻ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

❼ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

❽ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

해 설

❶ 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

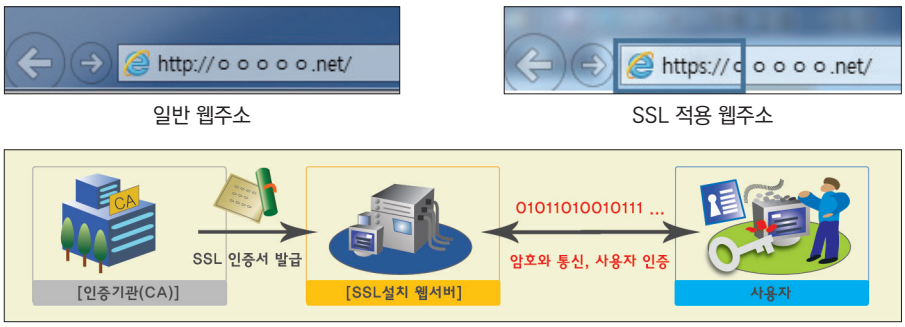
- 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
  - 고유식별정보는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다.
  - 비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
  - 바이오정보란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
  - 정보통신망이란 「전기통신기본법」제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

TIP
· 개인정보처리자는 자신이 제공하는 인터넷 홈페이지에서 이용자가 입력하는 고유식별정보, 비밀번호, 바이오정보를 암호화하여 송신하거나 전달하여야 한다.

- 정보통신망을 통하여 비밀번호를 송신하는 경우에는 SSL 등의 통신 암호 프로토콜이 탑재된 기술을 활용하여야 한다.

※ SSL(Secure Sockets Layer)은 웹 브라우저와 웹 서버간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜이다.

SSL 적용 예시



※ 개인정보 암호화 전송기술 사용 시 안전한 전송을 위해 잘 알려진 취약점(예시: Open SSL 사용 시 HeartBleed 취약점)들을 조치하고 사용 할 필요가 있다.

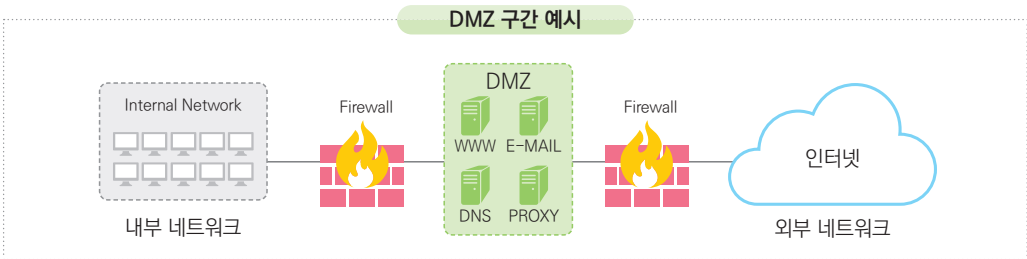
- 보조저장매체를 통해 고유식별정보, 비밀번호, 바이오정보를 전달하는 경우에도 암호화 하여야 하며, 이를 위해 다음과 같은 방법 등이 사용 될 수 있다.
  - 암호화 기능을 제공하는 보안 USB 등의 보조저장매체에 저장하여 전달
  - 해당 개인정보를 암호화 저장 한 후 보조저장매체에 저장하여 전달
- 고유식별정보, 비밀번호, 바이오정보를 제외한 개인정보(성명, 연락처 등)는 암호화 조치가 필수는 아니나, 개인정보의 위·변조 및 유·노출 등을 고려하여 가급적 암호화 조치를 권장한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 한다.
  - 비밀번호의 경우에는 복호화 되지 않도록 일방향(해쉬 함수) 암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서, 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다.
  - 바이오정보를 식별 및 인증 등의 업무에 활용하기 위하여 수집·이용하는 경우에는 암호화 조치를 하여야 하며 복호화가 가능한 양방향 암호화 저장을 할 수 있다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

- 인터넷 구간은 개인정보처리시스템과 인터넷이 직접 연결되어 있는 구간을 의미하고, DMZ 구간은 인터넷과 내부망 사이에 위치한 중간 지점 또는 인터넷 구간 사이에 위치한 중간 지점으로서 인터넷 구간에서 직접 접근이 가능한 영역을 말한다.(침입차단시스템 등으로 접근 제한 등을 수행하는 경우에도 해당) 또한, 내부망은 접근통제시스템 등에 의해 차단되어 외부에서 직접 접근이 불가능한 영역을 말한다.



- 인터넷 구간이나 DMZ 구간은 외부에서 직접 접근이 가능하므로 외부자의 침입을 받을 가능성이 있다. 이에 따라 DMZ 구간에 주민등록번호, 외국인등록번호, 운전면허번호, 여권번호 등의 고유식별정보를 저장하는 경우 암호화하여 저장해야 한다. 제2항에 따른 비밀번호 및 바이오정보를 저장하는 경우에도 암호화하여 저장해야한다.

④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과

부칙(제2016-35호, 2016. 9. 1.)

제2조(적용례) 영 제21조의2제2항에 따른 주민등록번호의 암호화 적용시기 이후에는 고유식별정보 중 주민등록번호는 제7조제4항을 적용하지 아니한다.

- 내부망에 주민등록번호를 저장하는 경우, 법 제24조의2, 동법 시행령 제21조의2에 따라 "개인정보 영향평가"나 암호화 미적용시 "위험도 분석"의 결과에 관계없이 암호화 하여야 한다. 이 경우에는 아래의 기간 이전까지 암호화 적용을 완료하여야 한다.

※ 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일

※ 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

「개인정보 보호법」제24조의2 제2항

제24조의2(주민등록번호 처리의 제한)

② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

「개인정보 보호법 시행령」제21조의2

제21조의2(주민등록번호 암호화 적용 대상 등)

① 법 제24조의2제2항에 따라 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다.

② 제1항의 개인정보처리자에 대한 암호화 적용 시기는 다음 각 호와 같다.

1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일
2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

③ 행정자치부장관은 기술적·경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.

● 내부망에 주민등록번호를 제외한 고유식별정보를 저장하는 경우에는 다음에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

- 「개인정보 보호법」제33조 및 시행령 제35조에 따라 영향평가의 대상이 되는 개인정보파일을 운용하는 공공기관은 해당 "개인정보 영향평가"의 결과

「개인정보 보호법」제33조제1항

제33조(개인정보 영향평가)

① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 행정자치부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정자치부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다.

「개인정보 보호법 시행령」제35조

제35조(개인정보 영향평가의 대상)

법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

- 공공기관 이외의 개인정보처리자는 암호화 미적용시 "위험도 분석"에 따른 결과

TIP · "개인정보 영향평가 수행 안내서" 및 "개인정보 위험도 분석 기준 및 해설서"는 개인정보보호 종합포털(http://www.privacy.go.kr)에서 다운로드 할 수 있다.

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

- 고유식별정보, 비밀번호, 바이오정보를 암호화 하는 경우에는 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

국내·외 암호 연구 관련 기관의 권고 암호 알고리즘 예시

분류	미국(NIST)	일본(CRYPTREC)	유럽(ECRYPT)	국내
대칭키 암호 알고리즘	AES-128/192/256 3TDEA	AES-128/192/256 3TDEA Camellia-128/192/256 MISTY1	AES-128/192/256 Blowfish KASUMI 3TDEA	SEED, HIGHT ARIA-128/192/256
공개키 암호 알고리즘 (메시지 암·복호화)	RSA (사용 권고하는 키길이 확인 필요)	RSAES-OAEP RSAES-PKCS1	RSAES-OAEP RSAES-PKCS1	RSAES-OAEP
일방향 암호 알고리즘	SHA-224/256/384/512	SHA-256/384/512	SHA-224/256/384/512 Whirlpool	SHA-224/256/384/512

· 국내·외 암호 연구 관련 기관에서 대표적으로 다루어지는 권고 암호 알고리즘만 표시('16.9월 기준)
· 권고 암호 알고리즘은 달라질 수 있으므로, 암호화 적용시 국내·외 암호 관련 연구기관에서 제시하는 최신 정보 확인 필요

TIP
· 안전한 암호알고리즘, 암호화 방식 등은 "개인정보의 암호화 조치 안내서"를 참조하고, 해당 자료는 개인정보보호 종합포털(http://www.privacy.go.kr)에서 다운로드 할 수 있다.
· 국내외 암호 연구 관련 기관은 한국인터넷진흥원(KISA)의 암호이용활성화 홈페이지(http://seed.kisa.or.kr)의 "암호 표준화 및 유관기관"에서도 확인 가능하다.
· 국가정보원 검증대상 암호 알고리즘 목록은 국가정보원 홈페이지에서 확인할 수 있다.

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

- 암호 키는 암호화된 데이터를 복호화 할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 매우 중요하며, 라이프사이클 단계별 암호 키 관리 절차를 수립·시행하여야 한다.

암호 키 관리 예시

1. 준비 단계: 암호 키가 사용되기 이전의 단계
   - 암호 키 생성
     · 암호 키 생성에 필요한 난수는 안전한 난수발생기(RNG)를 이용하여 생성
     · 비대칭키 알고리즘 키 생성 방식: 디지털 서명을 위한 키 쌍 생성, 키 설정을 위한 키 쌍 생성
     · 대칭키 알고리즘 방식: 미리 공유된 키, 패스워드, 다수의 암호 키를 이용한 키 생성 등
   - 암호 키 분배
     · 대칭키 알고리즘 키 분배 방식: 수동적 키 분배, 자동화된 키 전송 등
     · 비대칭키 알고리즘의 키 분배 방식
     · 기타 키 자료 생성 및 분배 방식: 영역 파라미터, 초기값, 공유된 비밀, RNG 시드, 다른 공개 및 비밀정보, 중간 값, 난수, 패스워드 등
2. 운영 단계: 암호 키가 암호 알고리즘 및 연산에 사용되는 단계
   - 암호 키의 유효기간동안 사용되는 키 자료들은 필요에 따라 장비 모듈에 보관되거나 별도의 저장 매체에 보관 등으로 저장해야 함
   - 암호 키는 하드웨어 손상 또는 소프트웨어 오류 등의 사유로 손상될 가능성이 있으므로 가용성 보장을 위해서는 키 백업 및 키 복구 등이 가능해야 함
   - 암호 키가 노출되거나 노출의 위협이 있는 경우 그리고 암호키 유효기간의 만료가 가까워지는 경우에는 암호 키를 다른 암호키로 안전하게 변경해야 함
3. 정지 단계: 암호 키가 더 이상 사용되지 않지만, 암호 키에 대한 접근은 가능한 단계
   - 암호 키 보관 및 복구
     · 암호 키는 수정이 불가한 상태이거나 새로운 보관 키를 이용하여 주기적으로 암호화
     · 운영 데이터와 분리되어 보관하며, 암호 정보의 사본들은 물리적으로 분리된 곳에 보관
     · 암호 키는 응용프로그램의 소스 프로그램 내에 평문으로 저장 금지
     · 암호화되는 중요한 정보에 대한 보관키는 백업되어야 하며, 사본은 다른 곳에 보관 등
   - 모든 개인키나 대칭키의 복사본이 더 이상 필요하지 않다면 즉시 파기하여야 함
   - 암호 키 손상시 유효기간 내에 키 자료를 제거하고, 보안 도메인에 속해있는 실체의 권한을 삭제하여 말소된 실체의 키 자료의 사용을 방지해야 함
4. 폐기 단계: 암호 키가 더 이상 사용될 수 없는 단계(폐기 또는 사고 상태)
   - 일반적으로 폐기 단계의 키 자료에 대한 모든 기록은 삭제(다만, 일부기관에서는 감사를 목적으로 특정 키 속성 유지가 필요할 수도 있음)
   - 폐기 상태의 암호 키와 사고 상태의 암호 키들의 특성에 대한 기록 유지 등

TIP · 개인정보보호 종합포털(http://www.privacy.go.kr)에서 제공하는 “개인정보의 암호화 조치 안내서” 그리고 암호이용활성화(http://seed.kisa.or.kr)에서 제공하는 “암호 키 관리 안내서” 등을 참고할 수 있다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

- 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하거나, 개인정보처리시스템으로부터 개인정보취급자의 업무용 컴퓨터, 모바일 기기에 내려 받아 저장하는 경우에는 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 이용하여 해당 파일을 암호화하여 불법적인 유·노출 및 접근 등으로부터 보호하여야 한다.

오피스에서 파일 암호화 설정방법

· 한컴 오피스: 파일 ➜ 다른이름으로 저장하기 ➜ 문서 암호 설정에서 암호 설정 가능
· MS 오피스: 파일 ➜ 다른이름으로 저장하기 ➜ 도구 ➜ 일반옵션에서 암호 설정 가능

암호화 적용 기준 요약표

<table>
<tr><th colspan="4">구 분</th><th>암호화 기준</th></tr>
<tr><td>정보통신망, 보조저장매체를 통한 송신 시</td><td colspan="3">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 송신</td></tr>
<tr><td rowspan="5">개인정보처리 시스템에 저장 시</td><td colspan="3">비밀번호</td><td>일방향(해쉬 함수) 암호화 저장</td></tr>
<tr><td colspan="3">바이오정보</td><td>암호화 저장</td></tr>
<tr><td rowspan="3">고유 식별정보</td><td colspan="2">주민등록번호</td><td>암호화 저장
※ 암호화 저장 시기는 제7조제4항 참고</td></tr>
<tr><td rowspan="2">여권번호, 외국인등록번호, 운전면허번호</td><td>인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)</td><td>암호화 저장</td></tr>
<tr><td>내부망에 저장</td><td>암호화 저장 또는 다음 항목에 따라 암호화 적용여부·적용범위를 정하여 시행
① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과
② 암호화 미적용시 위험도 분석에 따른 결과</td></tr>
<tr><td>업무용 컴퓨터, 모바일 기기에 저장시</td><td colspan="3">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 저장
※ 비밀번호는 일방향 암호화 저장</td></tr>
</table>

⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

안전조치 기준에 따른 적용 유형

제7조(개인정보의 암호화)		유형1 (완화)	유형2 (표준)	유형3 (강화)
항	호			
① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.		○	○	○
② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.		○	○	○
③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.		○	○	○
④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.	1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과	○	○	○
	2. 암호화 미적용시 위험도 분석에 따른 결과	○	○	○
부칙 제2조(적용례) 영 제21조의2제2항에 따른 주민등록번호의 암호화 적용시기 이후에는 고유식별정보 중 주민등록번호는 제7조제4항을 적용하지 아니한다.				
⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.		○	○	○
⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.				○
⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.		○	○	○
⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.				