구분	법/규정 명	규제 사항 예	추가
국내	개인정보보호법	제29조(안전조치의무) 개인정보처리자는 개인정보가 분실・도난・유출・변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적・관리적 및 물리적 조치를 하여야 한다. 제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 “고유식별정보”라 한다)를 처리할 수 없다. 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우 ② 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다. ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실・도난・유출・변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.	의료기관 정보보호 가이드라인 행안부_사업자의 개인정보보호 조치 기준
	산업기술유출방지법	제8조 (보호지침의 제정 등) ①지식경제부장관은 산업기술의 유출을 방지하고 산업기술을 보호하기 위하여 필요한 방법・절차 등에 관한 지침(이하 "보호지침"이라 한다)을 관계중앙행정기관의 장과 협의한 후 위원회의 심의를 거쳐 제정하고 이를 대상기관이 활용할 수 있도록 하여야 한다.	
	신용정보의이용및보호에관한법률	제19조(신용정보전산시스템의 안전보호) ① 신용정보회사등은 신용정보전산시스템(제25조제6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경・훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적・물리적・관리적 보안대책을 세워야 한다. ② 신용정보제공・이용자가 다른 신용정보제공・이용자 또는 신용조회회사와 서로 이 법에 따라 신용정보를 제공하는 경우에는 금융위원회가 정하여 고시하는 바에 따라 신용정보 보안관리 대책을 포함한 계약을 체결하여야 한다.	
	신용정보의이용및보호에관한법률시행령	제16조(기술적・물리적・관리적 보안대책의 수립) ① 법 제19조제1항에 따라 신용정보회사등은 신용정보전산시스템의 안전보호를 위하여 다음 각 호의 사항이 포함된 기술적・물리적・관리적 보안대책을 세워야 한다. 1. 신용정보에 제3자가 불법적으로 접근하는 것을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치・운영에 관한 사항 2. 신용정보전산시스템에 입력된 정보의 변경・훼손 및 파괴를 방지하기 위한 사항 3. 신용정보 취급・조회 권한을 직급별・업무별로 차등 부여하는 데에 관한 사항 및 신용정보 조회기록의 주기적인 점검에 관한 사항 4. 그 밖에 신용정보의 안정성 확보를 위하여 필요한 사항 ② 금융위원회는 제1항 각 호에 따른 사항의 구체적인 내용을 정하여 고시할 수 있다.	신용정보업감독규정 [별표3]기술적.물리적.관리적 보안대책 마련 기준
	위치정보의보호및이용등에관한법률	제16조(위치정보의 보호조치 등) ①위치정보사업자등은 위치정보의 누출, 변조, 훼손 등을 방지하기 위하여 위치정보의 취급・관리 지침을 제정하거나 접근권한자를 지정하는 등의 관리적 조치와 방화벽의 설치나 암호화 소프트웨어의 활용 등의 기술적 조치를 하여야 한다. 이 경우 관리적 조치와 기술적 조치의 구체적 내용은 대통령령으로 정한다. ②위치정보사업자등은 위치정보 수집・이용・제공사실 확인자료를 위치정보시스템에 자동으로 기록되고 보존되도록 하여야 한다. ③방송통신위원회는 위치정보를 보호하고 오용・남용을 방지하기 위하여 소속 공무원으로 하여금 제1항의 규정에 의한 기술적・관리적 조치의 내용과 제2항의 규정에 의한 기록의 보존실태를 대통령령이 정하는 바에 의하여 점검하게 할 수 있다.<개정 2008.2.29> ④제3항의 규정에 의하여 보존실태를 점검하는 공무원은 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 한다.	
	위치정보의보호및이용등에관한법률시행령	제20조(위치정보의 관리적・기술적 보호조치) ① 법 제16조제1항에 따른 관리적 조치에는 다음 각 호의 내용이 포함되어야 한다. 1. 위치정보관리책임자의 지정 2. 위치정보의 수집・이용・제공・파기 등 각 단계별 접근 권한자 지정 및 권한의 제한 3. 위치정보 취급자의 의무와 책임을 규정한 취급・관리 절차 및 지침 마련 4. 위치정보 제공사실 등을 기록한 취급대장의 운영・관리 5. 위치정보 보호조치에 대한 정기적인 자체 감사의 실시 ② 법 제16조제1항에 따른 기술적 조치에는 다음 각 호의 내용이 포함되어야 한다. 1. 위치정보 및 위치정보시스템의 접근권한을 확인할 수 있는 식별 및 인증 실시 2. 위치정보시스템에의 권한없는 접근을 차단하기 위한 암호화・방화벽 설치 등의 조치 3. 위치정보시스템에 대한 접근사실의 전자적 자동 기록・보존장치의 운영 4. 위치정보시스템의 침해사고 방지를 위한 보안프로그램 설치 및 운영	
	전자금융거래법	제22조(전자금융거래기록의 생성 및 보존) ①금융기관등은 전자금융거래의 내용을 추적・검색하거나 그 내용에 오류가 발생할 경우에 이를 확인하거나 정정할 수 있는 기록을 생성하여 5년의 범위 안에서 대통령령이 정하는 기간동안 보존하여야 한다. ②제1항의 규정에 따라 금융기관등이 보존하여야 하는 기록의 종류 및 보존방법은 대통령령으로 정한다.	전자금융감독규정 전자금융감독규정시행세칙

	정보통신기반보호법	제5조 (주요정보통신기반시설보호대책의 수립 등) ①주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제9조제1항의 규정에 의한 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립·시행하여야 한다. 제9조 (취약점의 분석·평가) ①관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.	
	정보통신망이용촉진및정보보호등에관한법률	제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다. 1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영 3. 접속기록의 위조·변조 방지를 위한 조치 4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치 6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치 제45조(정보통신망의 안정성 확보 등) ① 정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다. ② 방송통신위원회는 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치 및 안전진단의 방법·절차·수수료에 관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다. ③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. 1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치 2. 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치 3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치 4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치	
	정보통신망이용촉진및정보보호등에관한법률시행령	제15조(개인정보의 보호조치) ① 법 제28조제1항제1호에 따라 정보통신서비스 제공자등은 개인정보의 안전한 취급을 위하여 다음 각 호의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다. 1. 개인정보 관리책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항 2. 개인정보취급자의 교육에 관한 사항 3. 제2항부터 제5항까지의 규정에 따른 보호조치를 이행하기 위하여 필요한 세부 사항 ② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다. 1. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행 2. 개인정보처리시스템에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 및 침입탐지시스템의 설치·운영 3. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영 4. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치 ③ 법 제28조제1항제3호에 따라 정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 다음 각 호의 조치를 하여야 한다. 1. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독 2. 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관 ④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다. 1. 비밀번호 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)의 일방향 암호화 저장 2. 주민등록번호 및 계좌정보 등 금융정보의 암호화 저장 3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치 4. 그 밖에 암호화 기술을 이용한 보안조치 ⑤ 법 제28조제1항제5호에 따라 정보통신서비스 제공자등은 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신·점검하여야 한다. ⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.	방통위_개인정보의 기술적.관리적 보호조치 기준
	정보통신망이용촉진및정보보호등에관한법률시행규칙	제9조 (개인정보의 보호조치) ① 법 제28조제1항 및 제67조제1항에 따른 개인정보의 안전성 확보에 필요한 관리적 조치는 다음 각 호와 같다. 1. 개인정보의 안전한 취급을 위한 내부관리계획의 수립 및 시행 2. 개인정보 관리책임자의 의무와 책임을 규정한 내부 지침 마련 3. 개인정보의 안전한 보관을 위한 잠금장치 등 물리적 접근방지 조치 4. 개인정보보호를 위한 정기적인 자체 감사 실시 5. 그 밖에 개인정보의 안전성 확보에 필요한 관리적 보호조치 ② 법 제28조제1항 및 제67조제1항에 따른 개인정보의 안전성 확보에 필요한 기술적 조치는 다음 각 호와 같다. 1. 개인정보에 대한 접근 권한을 확인하기 위한 식별 및 인증 조치 2. 개인정보에 대한 권한 없는 접근을 차단하기 위한 암호화와 방화벽 설치 등의 조치 3. 접속기록의 위조·변조 방지를 위한 조치 4. 침해사고 방지를 위한 보안프로그램의 설치 및 운영	