韩国个人信息保护委员会告示《个人信息的安全性确保措施标准》全文韩中对照（非官方中文译文）

版本标识	pipc-safety-zh-20261016-08f19019
所译版本	告示第2026-9号，2026年7月1日公布，2026年7月1日起施行；共20条及附表1件
韩文原文取得	2026年11月8日，取自韩国国家法令信息中心（law.go.kr）
审校	由韩国律师李炫燮（Hyunsub Lee）审校，2026年10月16日
效力	非官方译文，不具有法律效力，以韩文原文为准。
更正及最新状态	依赖本文件之前，请在 https://datalaw.kr/zh/pipc-safety-standard/ 查看更正记录及是否有后续修正。更正后的译文使用新的版本标识。

书名号《》内的法令名称均指韩国法令，例如《个人信息保护法》指韩国的该法，而非中华人民共和国《个人信息保护法》。每一行对应一个条文本文、款、项或目，顺序与韩文原文相同；左栏为韩文原文，右栏为中文译文。条款栏注明附则另行规定施行时间的款、项。“#art-…”为网页上的行地址。发现译文错误，请将行地址和版本标识发送至 hyunsub.lee@seumlaw.com。

第一章 总则

제1장 총칙 · #ch-1

第1条（目的）

제1조(목적) · #art-1

第1条 제1조	이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제29조와 같은 법 시행령(이하 "영"이라 한다) 제16조제2항, 제30조 및 제30조의2에 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.	本标准的目的在于，依照《个人信息保护法》（以下称“法”）第29条及同法施行令（以下称“令”）第16条第2款、第30条及第30条之2，规定个人信息处理者在处理个人信息时，为使个人信息不发生丢失、被盗、泄露、伪造、变造或毁损而确保安全性所需的技术性、管理性及物理性安全措施的最低限度标准。

第2条（定义）

제2조(정의) · #art-2

第2条 제2조	이 기준에서 사용하는 용어의 뜻은 다음과 같다.	本标准中使用的用语，其含义如下：
第2条第1项 제2조제1호	1. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.	1. “个人信息处理系统”，是指数据库系统等为能够处理个人信息而系统性构建的系统。
第2条第2项 제2조제2호	2. "이용자"란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.	2. “用户”，是指使用《关于促进信息通信网利用及信息保护等的法律》第2条第1款第4项规定的信息通信服务提供者所提供的信息通信服务的人。
第2条第3项 제2조제3호	3. "접속기록"이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.	3. “访问记录”，是指对访问个人信息处理系统者访问个人信息处理系统后所执行的业务明细，以电子方式记录识别符、访问日期时间、访问地信息、所处理的信息主体信息、所执行业务等而形成的记录。此时，“访问”，是指与个人信息处理系统相连接、能够发送或接收数据的状态。
第2条第4项 제2조제4호	4. "정보통신망"이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 말한다.	4. “信息通信网”，是指《关于促进信息通信网利用及信息保护等的法律》第2条第1款第1项所称的，利用《电信事业法》第2条第2项规定的电信设备，或者运用电信设备与计算机及计算机利用技术，收集、加工、存储、检索、发送或接收信息的信息通信体系。

第2条第5项 제2조제5호	5. "P2P(Peer to Peer)"란 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.	5. “P2P（Peer to Peer）”，是指通过信息通信网，在没有服务器协助的情况下个人与个人直接连接并共享文件。
第2条第6项 제2조제6호	6. "공유설정"이란 컴퓨터 소유자의 파일을 타인이 조회 · 변경 · 복사 등을 할 수 있도록 설정하는 것을 말한다.	6. “共享设置”，是指将计算机所有者的文件设置为他人能够查询、变更、复制等。
第2条第7项 제2조제7호	7. "모바일 기기"란 무선망을 이용할 수 있는 스마트폰, 태블릿 컴퓨터 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.	7. “移动设备”，是指能够使用无线网络的智能手机、平板电脑等用于处理个人信息的便携式设备。
第2条第8项 제2조제8호	8. "비밀번호"란 정보주체 및 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 인증할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.	8. “密码”，是指信息主体及个人信息经办人员等访问个人信息处理系统或者管理信息通信网的系统等时，与识别符一同输入、为认证其为具有正当访问权限者而须传递给系统的固有字符串，且不向他人公开的信息。
第2条第9项 제2조제9호	9. "생체정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증 · 식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.	9. “生物特征信息”，是指指纹、面部、虹膜、静脉、声音、笔迹等关于个人身体、生理、行为特征的信息，且为认证、识别特定个人或者了解个人特征而通过一定技术手段处理的信息。
第2条第10项 제2조제10호	10. "생체인식정보"란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.	10. “生物识别信息”，是指生物特征信息中，以认证或识别特定个人为目的而通过一定技术手段处理的信息。
第2条第11项 제2조제11호	11. "인증정보"란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는데 사용되는 정보를 말한다.	11. “认证信息”，是指用于验证请求访问个人信息处理系统或者管理信息通信网的系统等者的身份的信息。
第2条第12项 제2조제12호	12. "내부망"이란 인터넷망 차단, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.	12. “内部网”，是指通过互联网阻断、访问控制系统等，使来自互联网区段的访问受到控制或被阻断的区段。
第2条第13项 제2조제13호	13. "위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별 · 평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.	13. “风险度分析”，是指为识别、评估可能对个人信息泄露产生影响的各种风险要素，并制定能够适当控制该风险要素的方案而进行综合分析的行为。
第2条第14项 제2조제14호	14. "보조저장매체"란 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 연결 · 분리할 수 있는 저장매체를 말한다.	14. “辅助存储介质”，是指移动式硬盘（HDD）、USB存储器等能够存储资料，且可与个人信息处理系统或者个人计算机等容易连接、分离的存储介质。

第二章 个人信息的安全性确保措施

제2장 개인정보의 안전성 확보조치 · #ch-2

第3条（安全措施的适用原则）

제3조(안전조치의 적용 원칙) · #art-3

第3条 제3조	개인정보처리자는 처리하는 개인정보의 보유 수, 유형 및 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는 개인정보의 안전성 확보에 필요한 조치를 적용하여야 한다.	个人信息处理者应当考虑所处理个人信息的持有数量、类型及对信息主体产生的影响等，采取符合自身环境的、确保个人信息安全性所需的措施。

第4条（内部管理计划的制定、实施及检查）

제4조(내부 관리계획의 수립 · 시행 및 점검) · #art-4

第4条第1款 제4조제1항	① 개인정보처리자는 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립 · 시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인 · 개인 · 단체의 경우에는 생략할 수 있다.	① 为使个人信息不发生丢失、被盗、泄露、伪造、变造或毁损，个人信息处理者应当通过内部决策程序，制定、实施包含下列各项事项的内部管理计划（但就未满1万名信息主体处理个人信息的小商工人、个人、团体，可以省略）：
第4条第1款第1项 제4조제1항제1호	1. 개인정보 보호 조직의 구성 및 운영에 관한 사항	1. 关于个人信息保护组织的构成及运营的事项；

第4条第1款第2项 제4조제1항제2호	2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항	2. 关于个人信息保护负责人的资格要件及指定的事项；
第4条第1款第3项 제4조제1항제3호	3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항	3. 关于个人信息保护负责人与个人信息经办人员的角色及责任的事项；
第4条第1款第4项 제4조제1항제4호	4. 개인정보취급자에 대한 관리 · 감독 및 교육에 관한 사항	4. 关于对个人信息经办人员的管理监督及教育的事项；
第4条第1款第5项 제4조제1항제5호	5. 접근 권한의 관리에 관한 사항	5. 关于访问权限管理的事项；
第4条第1款第6项 제4조제1항제6호	6. 접근통제에 관한 사항	6. 关于访问控制的事项；
第4条第1款第7项 제4조제1항제7호	7. 개인정보의 암호화 조치에 관한 사항	7. 关于个人信息加密措施的事项；
第4条第1款第8项 제4조제1항제8호	8. 접속기록 보관 및 점검에 관한 사항	8. 关于访问记录保管及检查的事项；
第4条第1款第9项 제4조제1항제9호	9. 악성프로그램 등 방지에 관한 사항	9. 关于防止恶意程序等的事项；
第4条第1款第10项 제4조제1항제10호	10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항	10. 关于为防止个人信息泄露、被盗等而进行的漏洞检查的事项；
第4条第1款第11项 제4조제1항제11호	11. 물리적 안전조치에 관한 사항	11. 关于物理性安全措施的事项；
第4条第1款第12项 제4조제1항제12호 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	12. 출력 · 복사시 안전조치에 관한 사항	12. 关于输出、复制时安全措施的事项；
第4条第1款第13项 제4조제1항제13호 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	13. 개인정보의 파기에 관한 사항	13. 关于个人信息销毁的事项；
第4条第1款第14项 제4조제1항제14호	14. 개인정보 유출사고 대응 계획 수립 · 시행에 관한 사항	14. 关于个人信息泄露事故应对计划的制定、实施的事项；
第4条第1款第15项 제4조제1항제15호	15. 위험 분석 및 관리에 관한 사항	15. 关于风险分析及管理的事项；
第4条第1款第16项 제4조제1항제16호	16. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항	16. 委托个人信息处理业务时，关于对受托方的管理及监督的事项；
第4条第1款第17项 제4조제1항제17호	17. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항	17. 关于个人信息内部管理计划的制定、变更及批准的事项；
第4条第1款第18项 제4조제1항제18호	18. 그 밖에 개인정보 보호를 위하여 필요한 사항	18. 其他为保护个人信息所需的事项。
第4条第2款 제4조제2항	② 개인정보처리자는 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다.	② 个人信息处理者应当规定下列各项事项，以个人信息保护负责人及个人信息经办人员为对象，根据事业规模、个人信息持有数量、业务性质等区别化地定期实施必要的教育：
第4条第2款第1项 제4조제2항제1호	1. 교육목적 및 대상	1. 教育目的及对象；
第4条第2款第2项 제4조제2항제2호	2. 교육 내용	2. 教育内容；
第4条第2款第3项 제4조제2항제3호	3. 교육 일정 및 방법	3. 教育日程及方法。
第4条第3款 제4조제3항	③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.	③ 第1款各项事项发生重要变更的，个人信息处理者应当立即予以反映，修改并实施内部管理计划，并管理其修改记录。

第4条第4款 제4조제4항	④ 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검 · 관리 하여야 한다.	④ 个人信息保护负责人应当每年1次以上对访问权限管理、访问记录保管及检查、加密措施等内部管理计划的履行状况进行检查、管理。

第5条（访问权限的管理）

제5조(접근 권한의 관리) · #art-5

第5条第1款 제5조제1항 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.	① 个人信息处理者应当在执行业务所需的最少限度范围内，区别授予对个人信息处理系统的访问权限。
第5条第2款 제5조제2항	② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.	② 个人信息经办人员或者个人信息经办人员的业务发生变更的，个人信息处理者应当毫不迟延地变更或注销个人信息处理系统的访问权限。
第5条第3款 제5조제3항	③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.	③ 个人信息处理者应当记录依照第1款及第2款进行的权限授予、变更或注销的明细，并将该记录至少保管3年。
第5条第4款 제5조제4항	④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.	④ 个人信息处理者发放能够访问个人信息处理系统的账户时，除有正当事由外，应当按每名个人信息经办人员分别发放账户，并使之不与其他个人信息经办人员共享。
第5条第5款 제5조제5항	⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.	⑤ 个人信息处理者应当安全地适用并管理个人信息经办人员或信息主体的认证手段。
第5条第6款 제5조제6항 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	⑥ 개인정보처리자는 정당한 권한을 가진 자만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.	⑥ 为使仅具有正当权限者能够访问个人信息处理系统，个人信息处理者应当采取认证失败达到一定次数以上时限制对个人信息处理系统的访问等必要措施。

第6条（访问控制）

제6조(접근통제) · #art-6

第6条第1款 제6조제1항	① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.	① 为防止通过信息通信网的非法访问及侵害事故，个人信息处理者应当采取下列各项安全措施：
第6条第1款第1项 제6조제1항제1호	1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한	1. 以互联网协议（IP）地址等限制对个人信息处理系统的访问权限，以限制未经授权的访问；
第6条第1款第2项 제6조제1항제2호	2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응	2. 分析访问过个人信息处理系统的互联网协议（IP）地址等，检测并应对个人信息泄露企图。
第6条第2款 제6조제2항 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	② 개인정보처리자는 개인정보처리시스템에 대한 정당한 접근 권한을 가진 자(다만, 정보주체는 제외한다)가 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.	② 对个人信息处理系统具有正当访问权限者（但信息主体除外）拟通过信息通信网从外部访问个人信息处理系统的，个人信息处理者应当适用证书、安保令牌、一次性密码等安全的认证手段。但处理非用户的信息主体的个人信息的个人信息处理系统，可以适用虚拟专用网络等安全的访问手段或者安全的认证手段。
第6条第3款 제6조제3항	③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.	③ 个人信息处理者应当对个人信息处理系统、个人信息经办人员的计算机及移动设备等采取措施，使所处理的个人信息不通过互联网网站、P2P、共享设置等向无权限者公开或泄露。
第6条第4款 제6조제4항	④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.	④ 为防止对个人信息处理系统的非法访问及侵害事故，个人信息处理者应当采取个人信息经办人员一定时间以上未进行业务处理时自动断开访问等必要措施。

第6条第5款 제6조제5항	⑤ 개인정보처리자는 업무용 모바일 기기의 분실 · 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.	⑤ 为防止因业务用移动设备丢失、被盗等导致个人信息泄露，个人信息处理者应当对该移动设备采取设置密码等保护措施。
第6条第6款 제6조제6항	⑥ 삭제	⑥ 删除

第6条之2（互联网的阻断措施等）

제6조의2(인터넷망의 차단 조치 등) · #art-6-2

第6条之2第1款 제6조의2제1항	① 전년도 말 기준 직전 3개월간 그 개인정보가 저장 · 관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 개인정보취급자의 컴퓨터 등에 대해 인터넷망 차단 조치를 하여야 한다. 다만, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성 · 운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하여야 한다.	① 以上一年度末为基准的前3个月期间，其个人信息被存储、管理的用户数日均达100万名以上的个人信息处理者，应当对属于下列各项之一的个人信息经办人员的计算机等采取互联网阻断措施。但利用《关于云计算发展及用户保护的法律》第2条第3项规定的云计算服务构建、运营个人信息处理系统的，应当采取除对该服务的访问外阻断互联网的措施：
第6条之2第1款第1项 제6조의2제1항제1호	1. 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자	1. 能够设定对个人信息处理系统的访问权限的个人信息经办人员；
第6条之2第1款第2项 제6조의2제1항제2호	2. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있는 개인정보취급자	2. 能够从个人信息处理系统下载或销毁个人信息的个人信息经办人员。
第6条之2第2款 제6조의2제2항	② 제1항제2호에도 불구하고 개인정보처리자는 내부 관리계획에서 정한 위험 분석 결과가 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 인터넷망 차단 조치를 하지 아니할 수 있다. 다만, 법 제23조에 따른 민감정보 또는 제7조제1항 · 제2항에 따른 개인정보를 다운로드 또는 파기할 수 있는 개인정보취급자의 컴퓨터 등에 대해서는 그러하지 아니하다.	② 尽管有第1款第2项的规定，内部管理计划中规定的风险分析结果属于下列各项之一的，个人信息处理者可以不采取第1款规定的互联网阻断措施。但对能够下载或销毁法第23条规定的敏感信息或者第7条第1款、第2款规定的个人信息的个人信息经办人员的计算机等，不在此限：
第6条之2第2款第1项 제6조의2제2항제1호	1. 위험 분석 결과 확인된 위험이 현저히 낮은 경우	1. 风险分析结果所确认的风险显著低的；
第6条之2第2款第2项 제6조의2제2항제2호	2. 위험 분석 결과 확인된 위험을 감소시킬 수 있는 보호조치를 적용한 경우. 이 경우 개인정보처리자는 [별표]에 따른 예시를 고려하여야 한다.	2. 已适用能够降低风险分析结果所确认的风险的保护措施的。此时，个人信息处理者应当考虑［附表］规定的示例。

第7条（个人信息的加密）

제7조(개인정보의 암호화) · #art-7

第7条第1款 제7조제1항	① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송 · 수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.	① 个人信息处理者存储密码、生物识别信息等认证信息，或者通过信息通信网发送、接收该等信息时，应当以安全的加密算法对其进行加密。但存储密码时，应当进行单向加密后存储，使之无法解密。
第7条第2款 제7조제2항	② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.	② 对属于下列各项的用户个人信息，个人信息处理者应当以安全的加密算法加密后存储：
第7条第2款第1项 제7조제2항제1호	1. 주민등록번호	1. 居民登记号码；
第7条第2款第2项 제7조제2항제2호	2. 여권번호	2. 护照号码；
第7条第2款第3项 제7조제2항제3호	3. 운전면허번호	3. 驾驶执照号码；
第7条第2款第4项 제7조제2항제4호	4. 외국인등록번호	4. 外国人登记号码；
第7条第2款第5项 제7조제2항제5호	5. 신용카드번호	5. 信用卡号码；

第7条第2款第6项 제7조제2항제6호	6. 계좌번호	6. 账户号码；
第7条第2款第7项 제7조제2항제7호	7. 생체인식정보	7. 生物识别信息。
第7条第3款 제7조제3항	③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.	③ 个人信息处理者按照下列各项方式存储非用户的信息主体的个人信息时，应当予以加密：
第7条第3款第1项 제7조제3항제1호	1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우	1. 在互联网区段及互联网区段与内部网之间的中间地带（DMZ：Demilitarized Zone）存储固有识别信息的；
第7条第3款第2项 제7조제3항제2호	2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)	2. 在内部网存储固有识别信息的（但存储居民登记号码以外的固有识别信息时，可以依照下列各目的标准确定并实施是否适用加密及其适用范围）：
第7条第3款第2项第1目 제7조제3항제2호가목	가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과	（1）属于法第33条规定的个人信息影响评估对象的公共机构，依照该个人信息影响评估的结果；
第7条第3款第2项第2目 제7조제3항제2호나목	나. 암호화 미적용시 위험도 분석에 따른 결과	（2）依照未适用加密时的风险度分析的结果。
第7条第4款 제7조제4항	④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송 · 수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.	④ 个人信息处理者通过信息通信网向互联网区段发送、接收个人信息时，应当以安全的加密算法对其进行加密。
第7条第5款 제7조제5항	⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.	⑤ 个人信息处理者将用户的个人信息或者非用户的信息主体的固有识别信息、生物识别信息存储于个人信息经办人员的计算机、移动设备及辅助存储介质等时，应当使用安全的加密算法加密后存储。
第7条第6款 제7조제6항	⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업 · 중견기업 · 공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업 · 단체에 해당하는 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립 · 시행하여야 한다.	⑥ 属于就10万名以上信息主体处理个人信息的大企业、中坚企业、公共机构，或者就100万名以上信息主体处理个人信息的中小企业、团体的个人信息处理者，为安全保管已加密的个人信息，应当制定、实施关于安全的加密密钥生成、利用、保管、分发及销毁等的程序。

第8条（访问记录的保管及检查）

제8조(접속기록의 보관 및 점검) · #art-8

第8条第1款 제8조제1항 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	① 개인정보처리자는 개인정보처리시스템에 접속한 자(다만, 정보주체는 제외한다)의 접속기록을 1년 이상 보관 · 관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관 · 관리하여야 한다.	① 个人信息处理者应当将访问过个人信息处理系统者（但信息主体除外）的访问记录保管、管理1年以上。但属于下列各项之一的，应当保管、管理2年以上：
第8条第1款第1项 제8조제1항제1호 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우	1. 属于处理5万名以上信息主体的个人信息的个人信息处理系统的；
第8条第1款第2项 제8조제1항제2호 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우	2. 属于处理固有识别信息或敏感信息的个人信息处理系统的；
第8条第1款第3项 제8조제1항제3호 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	3. 개인정보처리자로서 「전기통신사업법」제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우	3. 作为个人信息处理者，属于依照《电信事业法》第6条第1款进行登记或者依照同款但书进行申报的基干通信事业者的。

第8条第2款 제8조제2항 依附则（第2025-9号）第1条但书，自2026年11月1日起施行	② 개인정보처리자는 개인정보의 오 · 남용, 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손 등에 대응하기 위하여 개인정보취급자의 개인정보처리시스템에 대한 접속기록 및 개인정보 다운로드 상황을 확인하고 점검하는 주기 · 방법 · 사후조치절차 등을 내부 관리계획으로 정하고 이행하여야 한다.	② 为应对个人信息的误用、滥用，丢失、被盗、泄露、伪造、变造或毁损等，个人信息处理者应当以内部管理计划规定确认、检查个人信息经办人员对个人信息处理系统的访问记录及个人信息下载情况的周期、方法、事后措施程序等，并予以履行。
第8条第3款 제8조제3항	③ 개인정보처리자는 접속기록이 위 · 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.	③ 个人信息处理者应当采取安全保管访问记录的措施，使该访问记录不被伪造、变造及被盗、丢失。

第9条（防止恶意程序等）

제9조(악성프로그램 등 방지) · #art-9

第9条第1款 제9조제1항	① 개인정보처리자는 악성프로그램 등을 방지 · 치료할 수 있는 보안 프로그램을 설치 · 운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.	① 个人信息处理者应当安装、运营能够防止、清除恶意程序等的安保程序，并遵守下列各项事项：
第9条第1款第1项 제9조제1항제1호	1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지	1. 使用程序的自动更新功能，或者除有正当事由外每日实施1次以上更新等，保持最新状态；
第9条第1款第2项 제9조제1항제2호	2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치	2. 对所发现的恶意程序等采取删除等应对措施。
第9条第2款 제9조제2항	② 개인정보처리자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.	② 发布恶意程序相关警报，或者正在使用的应用程序或操作系统软件的制作厂商发布安保更新公告的，除有正当事由外，个人信息处理者应当立即实施相应的更新等。

第10条（物理性安全措施）

제10조(물리적 안전조치) · #art-10

第10条第1款 제10조제1항	① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립 · 운영하여야 한다.	① 个人信息处理者另设电算室、资料保管室等保管个人信息的物理保管场所的，应当制定、运营对其的出入控制程序。
第10条第2款 제10조제2항	② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.	② 个人信息处理者应当将含有个人信息的文书、辅助存储介质等保管于设有锁定装置的安全场所。
第10条第3款 제10조제3항	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.	③ 个人信息处理者应当制定用于控制含有个人信息的辅助存储介质移出、移入的安保对策。但不另行运营个人信息处理系统，而利用业务用计算机或者移动设备处理个人信息的，可以不适用。

第11条（防备灾害、灾难的安全措施）

제11조(재해 · 재난 대비 안전조치) · #art-11

第11条 제11조	10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업 · 중견기업 · 공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업 · 단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해 · 재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 한다.	属于就10万名以上信息主体处理个人信息的大企业、中坚企业、公共机构，或者就100万名以上信息主体处理个人信息的中小企业、团体的个人信息处理者，为在火灾、洪水、断电等灾害、灾难发生时保护个人信息处理系统，应当采取下列各项措施：
第11条第1项 제11조제1호	1. 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검	1. 制定危机应对手册等应对程序，并定期检查；
第11条第2项 제11조제2호	2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련	2. 制定个人信息处理系统备份及恢复的计划。

第12条（输出、复制时的安全措施）

제12조(출력 · 복사시 안전조치) · #art-12

第12条第1款 제12조제1항	① 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.	① 个人信息处理者从个人信息处理系统输出个人信息时（打印、画面显示、文件生成等），应当特定其用途，并根据用途使输出项目最小化。
第12条第2款 제12조제2항	② 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력 · 복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.	② 为安全管理含有个人信息的纸质印刷物、复制有个人信息的外部存储介质等个人信息的输出物、复制物，个人信息处理者应当采取所需的安全措施。

第13条（个人信息的销毁）

제13조(개인정보의 파기) · #art-13

第13条第1款 제13조제1항	① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.	① 个人信息处理者销毁个人信息时，应当采取下列各项中任一措施：
第13条第1款第1项 제13조제1항제1호	1. 완전파괴(소각 · 파쇄 등)	1. 完全破坏（焚烧、粉碎等）；
第13条第1款第2项 제13조제1항제2호	2. 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제	2. 利用专用消磁设备（利用磁场删除存储装置数据的设备）删除；
第13条第1款第3项 제13조제1항제3호	3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행	3. 执行初始化或覆盖写入，使数据无法恢复。
第13条第2款 제13조제2항	② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.	② 个人信息处理者仅销毁个人信息的一部分，难以用第1款的方法销毁时，应当采取下列各项措施：
第13条第2款第1项 제13조제2항제1호	1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독	1. 属于电子文件形态的：删除个人信息后进行管理及监督，使之无法恢复及再生；
第13条第2款第2项 제13조제2항제2호	2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제	2. 属于第1项以外的记录物、印刷物、书面文件及其他记录介质的：以遮盖、打孔等方式删除该部分。
第13条第3款 제13조제3항	③ 기술적 특성으로 제1항 및 제2항의 방법으로 파기하는 것이 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치를 하여야 한다.	③ 因技术特性以第1款及第2款的方法销毁存在显著困难的，应当将其处理为属于法第58条之2规定的信息，并采取措施使之无法恢复。

第三章 公共系统运营机构等的个人信息安全性确保措施

제3장 공공시스템 운영기관 등의 개인정보 안전성 확보조치 · #ch-3

第14条（公共系统运营机构的安全措施标准适用）

제14조(공공시스템운영기관의 안전조치 기준 적용) · #art-14

第14条第1款 제14조제1항	① 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템 중에서 개인정보보호위원회(이하 "보호위원회"라 한다)가 지정하는 개인정보처리시스템(이하 "공공시스템"이라 한다)을 운영하는 공공기관(이하 "공공시스템운영기관"이라 한다)은 제2장의 개인정보의 안전성 확보 조치 외에 이 장의 조치를 하여야 한다.	① 运营属于下列各项之一的个人信息处理系统中由个人信息保护委员会（以下称“保护委员会”）指定的个人信息处理系统（以下称“公共系统”）的公共机构（以下称“公共系统运营机构”），除第2章规定的个人信息安全性确保措施外，还应当采取本章规定的措施：
第14条第1款第1项 제14조제1항제1호	1. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 단일 시스템을 구축하여 다른 기관이 접속하여 이용할 수 있도록 한 단일접속 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우	1. 为支持2个以上机构的共同或类似业务而构建单一系统、使其他机构能够访问并利用的单一访问系统，且属于下列各目之一的：
第14条第1款第1项第1目 제14조제1항제1호가목	가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템	（1）处理100万名以上信息主体的个人信息的系统；
第14条第1款第1项第2目 제14조제1항제1호나목	나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템	（2）对个人信息处理系统的个人信息经办人员人数达200名以上的系统；

第14条第1款第1项第3目 제14조제1항제1호다목	다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템	（3）处理可能显著侵害信息主体私生活的敏感的个人信息的系统。
第14条第1款第2项 제14조제1항제2호	2. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 표준이 되는 시스템을 개발하여 다른 기관이 운영할 수 있도록 배포한 표준배포 시스템으로서 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우	2. 为支持2个以上机构的共同或类似业务而开发作为标准的系统、并分发给其他机构运营的标准分发系统，且用于面向国民服务的行政业务或者民愿业务处理的；
第14条第1款第3项 제14조제1항제3호	3. 기관의 고유한 업무 수행을 지원하기 위하여 기관별로 운영하는 개별 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우	3. 为支持机构固有业务的执行而按机构分别运营的个别系统，且属于下列各目之一的：
第14条第1款第3项第1目 제14조제1항제3호가목	가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템	（1）处理100万名以上信息主体的个人信息的系统；
第14条第1款第3项第2目 제14조제1항제3호나목	나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템	（2）对个人信息处理系统的个人信息经办人员人数达200名以上的系统；
第14条第1款第3项第3目 제14조제1항제3호다목	다. 「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템	（3）与《居民登记法》规定的居民登记信息系统连接运营的系统；
第14条第1款第3项第4目 제14조제1항제3호라목	라. 총 사업비가 100억원 이상인 시스템	（4）总事业费达100亿韩元以上的系统。
第14条第2款 제14조제2항	② 제1항에도 불구하고 보호위원회는 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템에 대하여는 공공시스템으로 지정하지 않을 수 있다.	② 尽管有第1款的规定，对属于下列各项之一的个人信息处理系统，保护委员会可以不指定为公共系统：
第14条第2款第1项 제14조제2항제1호	1. 체계적인 개인정보 검색이 어려운 경우	1. 难以进行系统性的个人信息检索的；
第14条第2款第2项 제14조제2항제2호	2. 내부적 업무처리만을 위하여 사용되는 경우	2. 仅用于内部业务处理的；
第14条第2款第3项 제14조제2항제3호	3. 그 밖에 개인정보가 유출될 가능성이 상대적으로 낮은 경우로서 보호위원회가 인정하는 경우	3. 其他个人信息泄露的可能性相对较低，且经保护委员会认可的。

第15条（公共系统运营机构的内部管理计划的制定、实施）

제15조(공공시스템운영기관의 내부 관리계획의 수립 · 시행) · #art-15

第15条 제15조	공공시스템운영기관은 공공시스템 별로 다음 각 호의 사항을 포함하여 내부 관리계획을 수립 · 시행하여야 한다.	公共系统运营机构应当按各公共系统，制定、实施包含下列各项事项的内部管理计划：
第15条第1项 제15조제1호	1. 영 제30조의2제4항에 따른 관리책임자(이하 "관리책임자"라 한다)의 지정에 관한 사항	1. 关于令第30条之2第4款规定的管理责任人（以下称“管理责任人”）的指定的事项；
第15条第2项 제15조제2호	2. 관리책임자의 역할 및 책임에 관한 사항	2. 关于管理责任人的角色及责任的事项；
第15条第3项 제15조제3호	3. 제4조제1항제3호에 관한 사항 중 개인정보취급자의 역할 및 책임에 관한 사항	3. 第4条第1款第3项事项中，关于个人信息经办人员的角色及责任的事项；
第15条第4项 제15조제4호	4. 제4조제1항제4호부터 제6호까지 및 제8호에 관한 사항	4. 关于第4条第1款第4项至第6项及第8项的事项；
第15条第5项 제15조제5호 依附则（第2026-9号）但书，自2027年1月1日起施行	5. 제16조부터 제18조까지에 관한 사항	5. 关于第16条至第18条的事项。

第16条（公共系统运营机构的访问权限的管理）

제16조(공공시스템운영기관의 접근 권한의 관리) · #art-16

第16条第1款 제16조제1항	① 공공시스템운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 한다.	① 公共系统运营机构拟授予、变更或注销对公共系统的访问权限时，应当与人事信息相连接。
第16条第2款 제16조제2항	② 공공시스템운영기관은 인사정보에 등록되지 않은 자에게 제5조제4항에 따른 계정을 발급해서는 안된다. 다만, 긴급상황 등 불가피한 사유가 있는 경우에는 그러하지 아니하며, 그 사유를 제5조제3항에 따른 내역에 포함하여야 한다.	② 公共系统运营机构不得向未在人事信息中登记者发放第5条第4款规定的账户。但存在紧急情况等不可避免的事由的，不在此限，且应当将该事由纳入第5条第3款规定的明细。
第16条第3款 제16조제3항	③ 공공시스템운영기관은 제5조제4항에 따른 계정을 발급할 때에는 개인정보 보호 교육을 실시하고, 보안 서약을 받아야 한다.	③ 公共系统运营机构发放第5条第4款规定的账户时，应当实施个人信息保护教育，并取得安保誓约。
第16条第4款 제16조제4항	④ 공공시스템운영기관은 정당한 권한을 가진 개인정보취급자에게만 접근 권한이 부여 · 관리되고 있는지 확인하기 위하여 제5조제3항에 따른 접근 권한 부여, 변경 또는 말소 내역 등을 반기별 1회 이상 점검하여야 한다.	④ 为确认访问权限是否仅授予具有正当权限的个人信息经办人员并受到管理，公共系统运营机构应当每半年1次以上检查第5条第3款规定的访问权限授予、变更或注销明细等。
第16条第5款 제16조제5항	⑤ 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 "공공시스템이용기관"이라 한다)은 소관 개인정보취급자의 계정 발급 등 접근 권한의 부여 · 관리를 직접하는 경우 제2항부터 제4항까지의 조치를 하여야 한다.	⑤ 访问公共系统并处理个人信息的机构（以下称“公共系统利用机构”）直接进行所管个人信息经办人员的账户发放等访问权限的授予、管理的，应当采取第2款至第4款规定的措施。

第17条（公共系统运营机构的访问记录的保管及检查）

제17조(공공시스템운영기관의 접속기록의 보관 및 점검) · #art-17

第17条第1款 제17조제1항	① 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용 · 남용 시도를 탐지하고 그 사유를 소명하도록 하는 등 필요한 조치를 하여야 한다.	① 应当采取以自动化方式分析公共系统访问记录等，检测非法的个人信息泄露及误用、滥用企图，并要求就该事由作出说明等必要措施。
第17条第2款 제17조제2항	② 공공시스템운영기관은 공공시스템이용기관이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능을 제공하여야 한다.	② 公共系统运营机构应当提供使公共系统利用机构能够直接检查所管个人信息经办人员访问记录的功能。

第18条（公共系统运营机构的漏洞检查及措施）

제18조(공공시스템운영기관의 취약점 점검 및 조치) · #art-18

第18条第1款 제18조제1항 依附则（第2026-9号）但书，自2027年1月1日起施行	① 공공시스템운영기관은 내부 관리계획에서 정한 취약점 점검을 공공시스템별로 연 1회 이상 실시하여야 한다.	① 公共系统运营机构应当按各公共系统每年1次以上实施内部管理计划中规定的漏洞检查。
第18条第2款 제18조제2항 依附则（第2026-9号）但书，自2027年1月1日起施行	② 공공시스템운영기관은 제1항에 따른 취약점 점검 외에 별도로 외부 전문기관 또는 외부 전문가에 의한 침투테스트를 공공시스템별로 연 1회 이상 실시하여야 한다.	② 除第1款规定的漏洞检查外，公共系统运营机构应当另行按各公共系统每年1次以上实施由外部专门机构或者外部专家进行的渗透测试。
第18条第3款 제18조제3항 依附则（第2026-9号）但书，自2027年1月1日起施行	③ 공공시스템운영기관은 제1항과 제2항에 따른 점검 결과 등에 따라 필요한 보완조치를 지체 없이 시행하여야 한다.	③ 公共系统运营机构应当根据第1款和第2款规定的检查结果等，毫不迟延地实施所需的弥补措施。

第19条（再审查期限）

제19조(재검토 기한) · #art-19

第19条 제19조	개인정보보호위원회는 「행정규제기본법」 제8조 및 「훈령 · 예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2023년 9월 15일을 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.	个人信息保护委员会应当依照《行政规制基本法》第8条及《关于训令、例规等的发布及管理的规定》，以2023年9月15日为基准，每满3年之时（指至每个第3年的9月14日为止），对本告示的妥当性进行审查，并采取改善等措施。

附则

附则 <第2020-2号, 2020. 8. 11.>

부칙 <제2020-2호,2020. 8. 11.> · #addendum-2020-2

이 고시는 고시한 날부터 시행한다.	本告示自告示之日起施行。

附则 <第2021-2号，2021. 9. 15.>

부칙 <제2021-2호, 2021. 9. 15.> · #addendum-2021-2

이 고시는 고시한 날부터 시행한다.	本告示自告示之日起施行。

附则 <第2023-6号，2023. 9. 22.>

부칙 <제2023-6호, 2023. 9. 22.> · #addendum-2023-6

이 고시는 발령한 날부터 시행한다. 다만, 다음 각 호의 개정규정은 각 호의 구분에 해당하는 개인정보처리자에 대해서는 2024년 9월 15일부터 시행한다.	本告示自发布之日起施行。但下列各项的修改规定，对属于各项所区分的个人信息处理者，自2024年9月15日起施行：
1. 제5조제6항, 제7조제6항, 제8조제2항, 제11조의 개정규정 : 종전의 「(개인정보보호위원회) 개인정보의 기술적 · 관리적 보호조치 기준」(개인정보보호위원회고시 제2021-3호) 적용대상인 개인정보처리자	1. 第5条第6款、第7条第6款、第8条第2款、第11条的修改规定：原《（个人信息保护委员会）个人信息的技术性、管理性保护措施标准》（个人信息保护委员会告示第2021-3号）的适用对象个人信息处理者
2. 제7조제4항, 제12조제2항의 개정규정 및 제5조제6항 중 정보주체에 관한 개정규정 : 종전의 「(개인정보보호위원회) 개인정보의 안전성 확보조치 기준」(개인정보보호위원회고시 제2021-2호) 적용대상인 개인정보처리자	2. 第7条第4款、第12条第2款的修改规定以及第5条第6款中关于信息主体的修改规定：原《（个人信息保护委员会）个人信息的安全性确保措施标准》（个人信息保护委员会告示第2021-2号）的适用对象个人信息处理者
3. 제14조부터 제17조까지의 개정규정 : 공공시스템운영기관과 공공시스템 이용기관	3. 第14条至第17条的修改规定：公共系统运营机构和公共系统利用机构

附则 <第2025-9号，2025. 10. 31.>

부칙 <제2025-9호, 2025. 10. 31.> · #addendum-2025-9

제1조(시행일) 이 고시는 발령한 날부터 시행한다. 다만, 제4조제1항 제12호 및 제13호, 제5조제1항 및 제6항, 제6조제2항, 제8조제1항 및 제2항은 발령한 날의 1년 후부터 시행한다.	第1条（施行日）本告示自发布之日起施行。但第4条第1款第12项及第13项、第5条第1款及第6款、第6条第2款、第8条第1款及第2款，自发布之日起1年后施行。

附则 <第2026-9号，2026. 7. 1.>

부칙 <제2026-9호, 2026. 7. 1.> · #addendum-2026-9

이 고시는 발령한 날 부터 시행한다. 다만, 제15조제5호 및 제18조는 2027년 1월 1일부터 시행한다.	本告示自发布之日起施行。但第15条第5项及第18条自2027年1月1日起施行。

附表

【附表】 能够降低风险的保护措施示例（与第6条之2相关）

[별표] 위험을 감소시킬 수 있는 보호조치 예시 (제6조의2 관련) · #annex

구분 **区分**	보호조치 예시 **保护措施示例**
1. 개인정보 파일을 다운로드 할 수 있는 개인정보취급자의 컴퓨터 등 1. 能够下载个人信息文件的个人信息经办人员的计算机等	◇ 개인정보처리시스템 접속 시 안전한 인증수단 적용 ◇ 개인정보 파일 저장 시 안전한 암호 알고리즘으로 암호화 ◇ 개인정보 다운로드 건수 제한 ◇ 개인정보 다운로드 권한을 가진 개인정보취급자 최소화 ◇ 개인정보 출력시 마스킹, 안심번호 등 표시제한 조치 적용 ◇ 访问个人信息处理系统时适用安全的认证手段 ◇ 存储个人信息文件时以安全的加密算法加密 ◇ 限制个人信息下载件数 ◇ 将具有个人信息下载权限的个人信息经办人员限定在最小范围 ◇ 输出个人信息时适用遮盖、安心号码等显示限制措施
2. 개인정보 파일을 파기할 수 있는 개인정보취급자의 컴퓨터 등 2. 能够销毁个人信息文件的个人信息经办人员的计算机等	◇ 개인정보 파기 권한을 가진 개인정보취급자 최소화 ◇ 개인정보 파기시 관리자 등으로부터 별도 승인을 받도록 설정 ◇ 将具有个人信息销毁权限的个人信息经办人员限定在最小范围 ◇ 设定为销毁个人信息时须另行取得管理员等的批准

구분 区分	보호조치 예시 保护措施示例
※ "예시"는 개인정보처리자가 개인정보에 대한 접근을 통제하기 위해 필요한 조치를 마련하는 과정에서 '필요한 조치'에 해당하는지를 판단할 때 적용해야 하는 안전조치 사례로, 실제 사례에서는 구체적 사실관계에 따라 필요한 부분을 선별적으로 적용할 수 있음 ※ “示例”，是指个人信息处理者在制定为控制对个人信息的访问所需的措施的过程中，判断是否属于‘所需的措施’时应当适用的安全措施实例；在实际案例中，可以根据具体事实关系选择性地适用所需的部分。	