ISO 27001:2013 정보보호 통제
Annex A control objectives and controls

A.5 보호 정책
Information security policies

A.5.1 정보보호를 위한 경영 방침
Management direction for information security

목적: 업무 요구사항과 관련 법률 및 규제에 따라 정보보호를 수행하도록 경영방침과 지원을 제공하기 위하여
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1 정보보호를 위한 정책
Policies for information security
정보보호를 위한 정책의 집합을 정의하고 경영진의 승인을 거쳐 직원 및 관련 외부자에게 공표하며 소통하여야 한다.
A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

A.5.1.2 정보보호 정책의 검토
Review of the policies for information security
정보보호 정책은 계획된 주기에 따라 또는 중대한 변경이 발생한 경우에 지속적인 적합성, 적절성, 효과성을 보장하기 위하여 검토하여야 한다.
The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

A.6 정보보호 조직
Organization of information security

A.6.1 내부 조직
Internal organization

목적: 조직 내에서 정보보호의 구현과 운영을 개시하고 통제하도록 관리 프레임워크를 수립하기 위하여
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

A.6.1.1 정보보호 역할 및 책임
Information security roles and responsibilities
모든 정보보호 책임을 정의하고 할당하여야 한다.
All information security responsibilities shall be defined and allocated.

A.6.1.2 직무 분리
Segregation of duties
조직의 자산에 인가되지 않거나 의도하지 않은 수정 또는 오용이 발생할 가능성을 줄이기 위하여 상충하는 직무와 책임 영역을 분리하여야 한다.
Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

A.6.1.3 관련 기관과의 연계
Contact with authorities
관련 기관에 대한 적절한 연계를 유지하여야 한다.
Appropriate contacts with relevant authorities shall be maintained.

A.6.1.4 전문가 그룹과의 연계
Contact with special interest groups
특별 관심 그룹 또는 전문가 보안 포럼 및 직능 단체와 적절한 연계를 유지하여야 한다.
Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A.6.1.5 프로젝트 관리에서의 정보보호
Information security in project management
프로젝트의 유형에 상관없이 프로젝트 관리 내에서 정보보호를 다루어야 한다.
Information security shall be addressed in project management, regardless of the type of the project.

A.6.2 모바일 기기 및 원격근무
Mobile devices and teleworking

목적: 원격근무와 모바일 기기의 사용에 따른 보안을 보장하기 위하여
Objective: To ensure the security of teleworking and use of mobile devices.

A.6.2.1 모바일 기기 정책
Mobile device policy
모바일 기기의 사용으로 인해 유발되는 위험을 관리하기 위하여 정책 및 이를 지원하는 보안 대책을 채택하여야 한다.
A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

A.6.2.2 원격근무
Teleworking
원격 근무지에서 접근, 처리, 저장하는 정보를 보호하기 위하여 정책을 수립하고 이를 지원하는 보안 대책을 구현하여야 한다.
A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

A.7 인적자원 보안
Human resource security

A.7.1 고용 전
Prior to employment

목적: 직원 및 계약직이 책임을 이해하고 주어진 역할에 적합한 자임을 보장하기 위하여
Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

A.7.1.1 적격심사
Screening
고용할 모든 후보자에 대한 배경 검증은 관련 법률, 규정, 윤리를 준수해야 하며, 업무 요구사항과 접근할 정보의 등급 및 예상되는 위험에 따라 적절하게 수행하여야 한다.
Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

A.7.1.2 고용 계약조건
Terms and conditions of employment
직원 및 계약직의 계약서에는 정보보호에 대한 개인과 조직의 책임을 명시하여야 한다.
The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.

A.7.2 고용 중
During employment

목적: 직원과 계약직이 자신의 정보보호 책임을 인식하고 충실하게 이행하도록 보장하기 위하여
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

A.7.2.1 경영진 책임
Management responsibilities
경영진은 모든 직원 및 계약직이 조직이 수립한 정책과 절차에 따라 정보보호를 수행하도록 요구하여야 한다.
Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

A.7.2.2 정보보호 인식, 교육, 훈련
Information security awareness, education and training
조직의 모든 직원과 관련 계약직은 자신의 직무 기능에 연관된 조직의 정책과 절차에 대해 적절한 인식 교육 및 훈련과 정기적인 갱신 교육을 받아야 한다.
All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

A.7.2.3 징계 처분
Disciplinary process
정보보호를 위반한 직원에 대한 조치를 취하도록 공식적인 징계 프로세스를 수립하여 배포하여야 한다.
There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

A.7.3 고용 종료 및 직무 변경
Termination and change of employment

목적: 직무 변경 또는 고용 종료 프로세스를 통해 조직의 이익을 보호하기 위하여
Objective: To protect the organization's interests as part of the process of changing or terminating employment.

A.7.3.1 고용 책임의 종료 또는 변경
Termination or change of employment responsibilities
고용이 종료되거나 직무가 변경된 이후에도 효력이 유지되어야 하는 정보보호의 책임과 의무를 정의하고 직원 또는 계약직에게 통지하여 시행하도록 하여야 한다.
Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

A.8 자산 관리
Asset management

A.8.1 자산에 대한 책임
Responsibility for assets

목적: 조직의 자산을 식별하고 적절한 보호 책임을 정의하기 위하여
Objective: To identify organizational assets and define appropriate protection responsibilities.

A.8.1.1 자산 목록
Inventory of assets
정보 및 정보처리 시설과 연관된 자산을 식별하고 자산에 대한 목록을 작성하여 유지하여야 한다.
Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

A.8.1.2 자산 소유권
Ownership of assets
목록으로 유지되는 자산은 소유자가 존재하여야 한다.
Assets maintained in the inventory shall be owned.

A.8.1.3 자산 이용
Acceptable use of assets
정보 및 정보처리 시설에 연관된 자산의 적절한 사용을 위한 규칙을 식별하고 문서화 및 구현하여야 한다.
Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

A.8.1.4 자산 반환
Return of assets
모든 직원과 외부 사용자는 고용이나 계약 또는 협약의 종료에 따라 자신이 소유한 조직의 자산을 모두 반환하여야 한다.
All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

A.8.2 정보 등급화
Information classification
목적: 조직에서의 중요성에 따라 정보에 적절한 보호 수준을 부여하도록 보장하기 위하여
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

A.8.2.1 정보 등급화
Classification of information
정보는 비인가 유출 또는 수정에 대한 법적 요구사항, 가치, 중요도, 민감도의 측면에서 등급화해야 한다.
Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

A.8.2.2 정보 표식
Labelling of information
조직에서 채택한 정보 등급화 체계에 따라 정보 표식을 위한 적절한 절차를 개발하고 구현하여야 한다.
An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

A.8.2.3 자산 취급
Handling of assets
조직에서 채택한 정보 등급화 체계에 따라 자산 취급 절차를 개발하고 구현하여야 한다.
Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

A.8.3 매체 취급
Media handling
목적: 매체에 저장된 정보의 비인가 유출, 수정, 삭제, 파손을 방지하기 위하여
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

A.8.3.1 이동식 매체 관리
Management of removable media
조직에서 채택한 정보 등급화 체계에 따라 이동식 매체의 관리를 위한 절차를 구현하여야 한다.
Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

A.8.3.2 매체 폐기
Disposal of media
더 이상 필요하지 않은 매체는 공식적인 절차를 통해 안전하게 폐기하여야 한다.
Media shall be disposed of securely when no longer required, using formal procedures.

A.8.3.3 물리적 매체 이송
Physical media transfer
정보를 포함한 매체는 운반 도중에 비인가 접근, 오용, 훼손으로부터 보호되어야 한다.
Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

A.9 접근통제
Access control
A.9.1 접근통제 업무 요구사항
Business requirements of access control
목적: 정보 및 정보처리 시설에 대한 접근을 제한하기 위하여
Objective: To limit access to information and information processing facilities.

A.9.1.1 접근통제 정책
Access control policy
업무 및 정보보호 요구사항을 기반으로 접근통제 정책을 수립하고 문서화 및 검토하여야 한다.
An access control policy shall be established, documented and reviewed based on business and information security requirements.

A.9.1.2 네트워크 및 네트워크 서비스 접근통제
Access to networks and network services
사용자는 특별히 인가된 네트워크 및 네트워크 서비스 에만 접근이 허용되어야 한다.
Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

A.9.2 사용자 접근관리
User access management
목적: 시스템과 서비스에 인가된 사용자 접근을 보장하고 비인가된 접근을 금지하기 위하여
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

A.9.2.1 사용자 등록 및 해지
User registration and de-registration
접근 권한의 할당이 가능하도록 공식적인 사용자 등록과 해지 프로세스를 구현하여야 한다.
A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

A.9.2.2 사용자 접근 권한설정
User access provisioning
모든 사용자 유형에 대한 접근 권한을 모든 시스템과 서비스에 할당하거나 폐지하기 위하여 공식적인 사용자 접근 권한설정 프로세스를 구현하여야 한다.
A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

A.9.2.3 특수 접근권한 관리
Management of privileged access rights
특수 접근권한에 대한 할당과 사용을 제한하고 통제하여야 한다.
The allocation and use of privileged access rights shall be restricted and controlled.

A.9.2.4 사용자 비밀 인증정보 관리
Management of secret authentication information of users
비밀 인증정보의 할당은 공식적인 관리 프로세스를 거쳐 통제하여야 한다.
The allocation of secret authentication information shall be controlled through a formal management process.

A.9.2.5 사용자 접근권한 검토
Review of user access rights
자산 소유자는 정기적으로 사용자 접근권한을 검토하여야 한다.
Asset owners shall review users' access rights at regular intervals.

A.9.2.6 접근권한 제거 또는 조정
Removal or adjustment of access rights
정보 및 정보처리 시설에 대한 모든 직원과 외부 사용자의 접근권한은 고용, 계약, 협약의 종료에 따라 제거하거나 변경된 상황에 따라 조정하여야 한다.
The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9.3 사용자 책임
User responsibilities
목적: 사용자가 자신의 인증정보를 보호할 책임을 부과하기 위하여
Objective: To make users accountable for safeguarding their authentication information.

A.9.3.1 기밀 인증정보 사용
Use of secret authentication information
사용자에게 비밀 인증정보의 사용 시 조직의 실무를 따르도록 요구하여야 한다.
Users shall be required to follow the organization's practices in the use of secret authentication information.

A.9.4 시스템 및 애플리케이션 접근통제
System and application access control
목적: 시스템과 애플리케이션에 대한 비인가 접근을 방지하기 위하여
Objective: To prevent unauthorized access to systems and applications.

A.9.4.1 정보 접근제한
Information access restriction
접근통제 정책에 따라 정보와 응용 시스템 기능에 대한 접근을 제한하여야 한다.
Access to information and application system functions shall be restricted in accordance with the access control policy.

A.9.4.2 안전한 로그인 절차
Secure log-on procedures
접근통제 정책에서 요구하는 경우에 시스템과 애플리케이션에 대한 접근은 안전한 로그인 절차에 따라

A.9.4.3 패스워드 관리 시스템
Password management system
패스워드 관리 시스템은 대화식으로 양질의 패스워드를 보장하여야 한다.
Password management systems shall be interactive and shall ensure quality passwords.

A.9.4.4 특수 유틸리티 프로그램 사용
Use of privileged utility programs
시스템과 애플리케이션의 통제를 초월할 수 있는 유틸리티 프로그램은 제한적으로 사용하고 철저히 통제하여야 한다.
The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

A.9.4.5 프로그램 소스코드 접근통제
Access control to program source code
프로그램 소스 코드에 대한 접근은 제한하여야 한다.
Access to program source code shall be restricted.

A.10 암호화
Cryptography
A.10.1 암호 통제
Cryptographic controls
목적: 정보에 대한 기밀성, 인증, 무결성을 보호하도록 암호화의 적절하고 효과적인 사용을 보장하기 위하여
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.10.1.1 암호 통제 사용 정책
Policy on the use of cryptographic controls
정보의 보호를 위한 암호 통제의 사용 정책을 개발하고 구현하여야 한다.
A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

A.10.1.2 키 관리
Key management
전체 생명주기에 걸쳐 암호키의 사용, 보호, 수명에 대한 정책을 개발하고 구현하여야 한다.
A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

A.11 물리적 및 환경적 보안
Physical and environmental security
A.11.1 보안 구역
Secure areas
목적: 조직의 정보 및 정보처리 시설에 대한 비인가된 물리적 접근, 파손, 간섭을 방지하기 위하여
Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

A.11.1.1 물리적 보안 경계
Physical security perimeter
기밀 또는 중요 정보와 정보처리 시설을 포함한 구역을 보호하기 위하여 보안 경계를 정의하고 이용하

여야 한다.
Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

A.11.1.2 물리적 출입 통제
Physical entry controls
보안 구역은 인가된 인력만 접근이 허용됨을 보장하기 위하여 적절한 출입 통제로 보호하여야 한다.
Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

A.11.1.3 사무 공간 및 시설 보안
Securing offices, rooms and facilities
사무 공간 및 시설에 대한 물리적 보안을 설계하고 적용하여야 한다.
Physical security for offices, rooms and facilities shall be designed and applied.

A.11.1.4 외부 및 환경 위협에 대비한 보호
Protecting against external and environmental threats
자연 재해, 악의적인 공격 또는 사고에 대비한 물리적 보호를 설계하고 적용하여야 한다.
Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

A.11.1.5 보안 구역 내 작업
Working in secure areas
보안 구역 내에서의 작업을 위한 절차를 설계하고 적용하여야 한다.
Procedures for working in secure areas shall be designed and applied.

A.11.1.6 배송 및 하역 구역
Delivery and loading areas
배송 및 하역 구역과 같이 비인가자가 구내로 들어올 수 있는 접근 장소는 통제하여야 하며, 비인가 접근을 피하기 위하여 정보처리 시설에서 가능한 고립시켜야 한다.
Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

A.11.2 장비
Equipment
목적: 자산의 분실, 손상, 도난, 훼손 및 조직의 운영 중단을 방지하기 위하여
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

A.11.2.1 장비 배치 및 보호
Equipment siting and protection
장비는 환경적 위협과 유해요소, 비인가 접근의 가능성을 감소시킬 수 있도록 배치하고 보호하여야 한다.
Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

A.11.2.2 지원 설비
Supporting utilities
지원 설비의 장애로 인한 전력 중단이나 기타 저해요인으로부터 장비를 보호하여야 한다.
Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

A.11.2.3 배선 보안
Cabling security
데이터를 전송하거나 정보 서비스를 지원하는 전력 및 통신 배선을 도청, 간섭, 파손으로부터 보호하여야 한다.
Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

A.11.2.4 장비 유지보수
Equipment maintenance
장비는 지속적인 가용성과 무결성을 보장하도록 정확하게 유지하여야 한다.
Equipment shall be correctly maintained to ensure its continued availability and integrity.

A.11.2.5 자산 반출
Removal of assets
장비, 정보, 소프트웨어는 사전 승인 없이 외부로 반출 되지 않도록 해야 한다.
Equipment, information or software shall not be taken off-site without prior authorization.

A.11.2.6 구외 장비 및 자산 보안
Security of equipment and assets off-premises
조직 외부에서의 작업으로 인한 다양한 위험을 고려하여 구외(off-site) 자산에 보안을 적용하여야 한다.
Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.

A.11.2.7 장비 안전 폐기 및 재사용
Secure disposal or reuse of equipment
저장 매체를 포함하고 있는 모든 장비는 폐기 또는 재사용하기 전에 기밀 데이터와 라이선스 소프트웨어를 삭제하거나 안전한 덮어쓰기 처리를 보장하기 위하여 검증하여야 한다.
All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

A.11.2.8 방치된 사용자 장비
Unattended user equipment
사용자는 방치된 장비에 대한 적절한 보호를 보장하여야 한다.
Users shall ensure that unattended equipment has appropriate protection.

A.11.2.9 책상 정리 및 화면보호 정책
Clear desk and clear screen policy
서류와 이동식 저장 매체를 대상으로 한 책상 정리 정책 및 정보처리 시설에 대한 화면보호 정책을 적용하여야 한다.
A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

A.12 운영 보안
Operations security
A.12.1 운영 절차 및 책임
Operational procedures and responsibilities
목적: 정보처리 시설의 정확하고 안전한 운영을 보장하기 위하여
Objective: To ensure correct and secure operations of information processing facilities.

A.12.1.1 운영 절차 문서화
Documented operating procedures
운영 절차를 문서화하고 필요한 모든 사용자가 이용할 수 있도록 하여야 한다
.Operating procedures shall be documented and made available to all users who need them.

A.12.1.2 변경 관리
Change management
정보보호에 영향을 주는 조직, 업무 프로세스, 정보처리 시설, 시스템의 변경을 통제하여야 한다.
Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

A.12.1.3 용량 관리
Capacity management
필요한 시스템 성능을 보장하기 위하여 자원의 사용을 모니터링 및 조절하고 향후 용량 요구사항을 예측하여야 한다.
The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

A.12.1.4 개발, 시험, 운영 환경 분리
Separation of development, testing and operational environments
운영 환경에 대한 비인가 접근 또는 변경의 위험을 감소시키기 위하여 개발 및 시험과 운영 환경은 분리하여야 한다.
Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

A.12.2 악성코드 방지
Protection from malware
목적: 정보 및 정보처리 시설이 악성코드로부터 보호됨을 보장하기 위하여
Objective: To ensure that information and information processing facilities are protected against malware.

A.12.2.1 악성코드 통제
Controls against malware
악성코드로부터 보호하기 위하여 탐지, 예방, 복구 통제를 구현하고 적절한 사용자 인식 교육을 연계하여야한다.
Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

A.12.3 백업
Backup
목적: 데이터의 손실을 방지하기 위하여
Objective: To protect against loss of data.

A.12.3.1 정보 백업
Information backup
합의된 백업 정책에 따라 주기적으로 정보, 소프트웨어, 시스템 이미지에 대한 백업 복사본을 생성하고 시험하여야 한다.
Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

A.12.4 로그기록 및 모니터링
Logging and monitoring
목적: 이벤트를 기록하고 증거를 생성하기 위하여
Objective: To record events and generate evidence.

A.12.4.1 이벤트 로그기록
Event logging
사용자 활동, 예외, 고장, 정보보호 이벤트를 기록하는 이벤트 로그를 생성하고 보존하며 주기적으로 검토하여야 한다.
Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.12.4.2 로그 정보 보호
Protection of log information
로그기록 설비와 로그 정보를 변조 및 비인가 접근으로부터 보호하여야 한다.
Logging facilities and log information shall be protected against tampering and unauthorized access.

A.12.4.3 관리자 및 운영자 로그
Administrator and operator logs
시스템 관리자와 시스템 운영자의 활동을 기록하고 로그를 보호하여 주기적으로 검토하여야 한다.
System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

A.12.4.4 시각 동기화
Clock synchronisation
조직 또는 보안 영역 내에서 모든 관련 정보처리 시스템의 시각은 동일한 출처의 참조 시간으로 동기화하여야 한다.
The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.

A.12.5 운영 소프트웨어 통제
Control of operational software
목적: 운영 시스템의 무결성을 보장하기 위하여
Objective: To ensure the integrity of operational systems.

A.12.5.1 운영 시스템 소프트웨어 설치
Installation of software on operational systems
운영 시스템 상의 소프트웨어 설치를 통제하기 위한 절차를 구현하여야 한다.
Procedures shall be implemented to control the installation of software on operational systems.

A.12.6 기술적 취약점 관리
Technical vulnerability management
목적: 기술적 취약점의 악용을 방지하기 위하여
Objective: To prevent exploitation of technical vulnerabilities.

A.12.6.1 기술적 취약점 관리
Management of technical vulnerabilities
사용 중인 정보시스템의 기술 취약점 정보를 적시에 수집하고, 해당 취약점에 대한 조직의 노출 정도를 평가하여 관련 위험을 해결할 수 있는 적절한 조치를 취해야 한다.
Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A.12.6.2 소프트웨어 설치 제한
Restrictions on software installation
사용자의 소프트웨어 설치를 제한하는 규정을 수립하고 구현하여야 한다.
Rules governing the installation of software by users shall be established and implemented.

A.12.7 정보시스템 감사 고려사항
Information systems audit considerations
목적: 운영 시스템에 대한 감사 활동의 영향을 최소화하기 위하여
Objective: To minimise the impact of audit activities on operational systems.

A.12.7.1 정보시스템 감사 통제
Information systems audit controls
운영 시스템의 검증에 필요한 감사 요구사항과 활동은 업무 프로세스의 중단을 최소화하도록 신중하게 계획하고 합의를 거쳐야 한다.
Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

A.13 통신 보안
Communications security
A.13.1 네트워크 보안 관리
Network security management
목적: 네트워크 상의 정보와 이를 지원하는 정보처리 시스템의 보호를 보장하기 위하여
Objective: To ensure the protection of information in networks and its supporting information processing facilities.

A.13.1.1 네트워크 통제
Network controls
시스템과 애플리케이션에서 처리되는 정보를 보호하기 위하여 네트워크를 관리하고 통제하여야 한다.
Networks shall be managed and controlled to protect information in systems and applications.

A.13.1.2 네트워크 서비스 보안
Security of network services
내부 또는 외부에서 제공하는 모든 네트워크 서비스의 보안 메커니즘, 서비스 수준, 관리 요구사항을 식별하고 네트워크 서비스 협약에 포함시켜야 한다.
Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

A.13.1.3 네트워크 분리
Segregation in networks
정보 서비스, 사용자, 정보시스템을 그룹화하여 네트워크 상에서 분리하여야 한다.
Groups of information services, users and information systems hall be segregated on networks.

A.13.2 정보 전송
Information transfer
목적: 조직 내부에서 또는 외부자에게 전송되는 정보의 보안을 유지하기 위하여
Objective: To maintain the security of information transferred within an organization and with any external entity.

A.13.2.1 정보 전송 정책 및 절차
Information transfer policies and procedures
모든 유형의 통신 시설을 거치는 정보의 전송을 보호하기 위하여 공식적인 전송 정책, 절차, 통제를 마련하여야 한다.
Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

A.13.2.2 정보 전송 협약
Agreements on information transfer
조직과 외부자 간의 업무 정보를 안전하게 전송하기 위한 협약을 체결하여야 한다.
Agreements shall address the secure transfer of business information between the organization and external parties.

A.13.2.3 전자 메시지 교환
Electronic messaging
전자적인 메시지 교환에 포함된 정보는 적절하게 보호하여야 한다.
Information involved in electronic messaging shall be appropriately protected.

A.13.2.4 기밀유지 협약
Confidentiality or nondisclosure agreements
정보보호에 대한 조직의 요구를 반영한 기밀유지협약 및 비밀유지서약 요구사항을 식별하고 주기적으로 검토 및 문서화하여야 한다.
Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.

A.14 시스템 도입, 개발, 유지보수
System acquisition, development and maintenance
A.14.1 정보시스템 보안 요구사항
Security requirements of information systems
목적: 공중망을 통해 서비스를 제공하는 정보시스템에 대한 요구사항도 포함하여 정보시스템의 전체 생명주기에 걸쳐 정보보호가 필수적인 부분임을 보장하기 위하여
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A.14.1.1 정보보호 요구사항 분석 및 명세
Information security requirements analysis and specification
정보보호 관련 요구사항을 신규 정보시스템의 요구사항이나 기존 정보시스템의 개선사항에 포함시켜야 한다.
The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

A.14.1.2 공중망 응용 서비스 보안
Securing application services on public networks
공중망을 통해 전달되는 응용 서비스의 정보는 부정행위, 계약 분쟁, 비인가 유출 및 수정으로부터 보호하여야 한다.
Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

A.14.1.3 응용 서비스 거래 보호
Protecting application services transactions
응용 서비스 거래의 정보는 불완전 전송, 경로 이탈, 비인가 메시지 변경, 비인가 노출, 비인가 메시지 중복, 재사용을 방지하도록 보호하여야 한다.
Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

A.14.2 개발 및 지원 프로세스 보안
Security in development and support processes
목적: 정보시스템 개발 생명주기 내에 정보보호를 설계하고 구현함을 보장하기 위하여
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

A.14.2.1 개발 보안 정책
Secure development policy
조직 내에서 소프트웨어와 시스템의 개발을 위한 규칙을 수립하고 적용하여야 한다.
Rules for the development of software and systems shall be established and applied to developments within the organization.

A.14.2.2 시스템 변경 통제 절차
System change control procedures
공식적인 변경 통제 절차를 사용하여 개발 생명주기 내에서 시스템의 변경을 통제하여야 한다.
Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

A.14.2.3 운영 플랫폼 변경 후 애플리케이션 기술적 검토
Technical review of applications after operating platform changes
운영 플랫폼이 변경되면 조직의 운영이나 보안에 부정적인 영향을 미치지 않음을 보장하기 위하여 업무에 중요한 애플리케이션을 검토하고 시험하여야 한다.
When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

A.14.2.4 소프트웨어 패키지 변경 제한
Restrictions on changes to software packages
소프트웨어 패키지에 대한 변경은 반드시 필요한 경우에만 제한적으로 허용하고 모든 변경을 엄격하게 통제하여야 한다.
Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

A.14.2.5 시스템 보안 공학 원칙
Secure system engineering principles
시스템 보안 공학을 위한 원칙을 수립하여 문서화하고 유지하며 모든 정보시스템의 구현에 적용하여야 한다.
Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

A.14.2.6 개발 환경 보안
Secure development environment
조직은 시스템의 전체 개발 생명주기를 포괄하는 시스템 개발 및 통합을 위해 안전한 개발 환경을 수립하고 적절히 보호하여야 한다.
Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

A.14.2.7 외주 개발
Outsourced development

조직은 외주 시스템 개발 활동을 감독하고 모니터링 하여야 한다.
The organization shall supervise and monitor the activity of outsourced system development.

A.14.2.8 시스템 보안 시험
System security testing
개발 기간 동안에 보안 기능의 시험을 수행하여야 한다.
Testing of security functionality shall be carried out during development.

A.14.2.9 시스템 인수 시험
System acceptance testing
신규 정보시스템, 업그레이드, 신규 버전에 대한 인수
시험 프로그램과 관련 기준을 수립하여야 한다.
Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

A.14.3 시험 데이터
Test data
목적: 시험에 사용되는 데이터의 보호를 보장하기 위하여
Objective: To ensure the protection of data used for testing.

A.14.3.1 시험 데이터 보호
Protection of test data
시험 데이터를 신중하게 선택하여 보호하고 통제하여야 한다.
Test data shall be selected carefully, protected and controlled.

A.15 공급자 관계
Supplier relationships
A.15.1 공급자 관계 정보보호
Information security in supplier relationships
목적: 공급자가 접근할 수 있는 조직 자산에 대한 보호를 보장하기 위하여
Objective: To ensure protection of the organization's assets that is accessible by suppliers.

A.15.1.1 공급자 관계 정보보호 정책
Information security policy for supplier relationships
조직 자산에 대한 공급자 접근과 연관된 위험을 감소시키기 위한 정보보호 요구사항은 공급자와 합의를 거쳐 문서화하여야 한다.
Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

A.15.1.2 공급자 협약 내 보안 명시
Addressing security within supplier agreements
모든 관련 정보보호 요구사항을 수립하여 조직 정보에 대한 접근, 처리, 저장, 통신을 수행하거나 IT 기반 구성요소를 제공하는 공급자와 합의하여야 한다.
All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

A.15.1.3 정보통신기술 공급망
Information and communication technology supply chain
공급자와 관련된 협약에는 정보통신기술 서비스와 제품 공급망에 연관된 정보보호 위험을 다루는 요구사항을 포함하여야 한다.
Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

A.15.2 공급자 서비스 전달 관리
Supplier service delivery management
목적: 공급자 협약에 따라 합의된 수준의 정보보호와 서비스 전달을 유지하기 위하여
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A.15.2.1 공급자 서비스 모니터링 및 검토
Monitoring and review of supplier services
조직은 공급자의 서비스 전달을 주기적으로 모니터링 하고 검토 및 감사를 수행하여야 한다.
Organizations shall regularly monitor, review and audit supplier service delivery.

A.15.2.2 공급자 서비스 변경 관리
Managing changes to supplier services
기존 정보보호 정책, 절차, 통제의 유지관리와 개선을 포함 공급자의 서비스 제공에 대한 변경은 업무 정보, 시스템, 프로세스의 중요성과 위험의 재평가를 감안하여 관리하여야 한다.
Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

A.16 정보보호 사고 관리
Information security incident management
A.16.1 정보보호 사고 관리 및 개선
Management of information security incidents and improvements
목적: 보안 이벤트와 약점에 대한 의사소통을 포함하여 정보보호 사고의 일관되고 효과적인 접근을 보장하기 위하여
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A.16.1.1 책임 및 절차
Responsibilities and procedures
정보보호 사고에 대한 신속하고 효과적이며 순차적인 대응을 보장하기 위하여 관리 책임과 절차를 수립하여야 한다.
Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

A.16.1.2 정보보호 이벤트 보고
Reporting information security events
적절한 관리 채널을 통해 가능한 신속하게 정보보호 이벤트를 보고하여야 한다.
Information security events shall be reported through appropriate management channels as quickly as possible.

A.16.1.3 정보보호 약점 보고
Reporting information security weaknesses
조직의 정보시스템과 서비스를 사용하는 직원 및 계약자는 시스템 또는 서비스에서 정보보호 약점을 발견하거나 의심되는 경우에 주의 깊게 살펴서 보고하여야한다.
Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

A.16.1.4 정보보호 이벤트 평가 및 의사결정
Assessment of and decision on information security events
정보보호 이벤트를 평가하고 정보보호 사고로 분류할지 여부를 결정하여야 한다.
Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

A.16.1.5 정보보호 사고 대응
Response to information security incidents
정보보호 사고는 문서화된 절차에 따라 대응하여야 한다.
Information security incidents shall be responded to in accordance with the documented procedures.

A.16.1.6 정보보호 사고로부터 학습
Learning from information security incidents
정보보호 사고를 분석하고 해결하는 과정에서 습득한 지식은 추후 사고의 가능성 또는 영향을 줄이는데 사용하여야 한다
Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents..

A.16.1.7 증거 수집
Collection of evidence
조직은 증거로 활용할 수 있는 정보를 식별, 수집, 획득, 보존하기 위한 절차를 정의하고 적용하여야 한다.
The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

A.17 업무연속성 관리의 정보보호 측면
Information security aspects of business continuity management
A.17.1 정보보호 연속성
Information security continuity
목적: 조직의 업무연속성 관리체계 내에 정보보호 연속성을 포함시켜야 한다.
Objective: Information security continuity shall be embedded in the organization's business continuity management systems.

A.17.1.1 정보보호 연속성 계획
Planning information security continuity
조직은 위기 또는 재난과 같이 어려운 상황에서 정보보호와 정보보호 관리의 연속성에 대한 요구사항을 결정하여야 한다.
The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

A.17.1.2 정보보호 연속성 구현
Implementing information security continuity
조직은 어려운 상황에서 정보보호에 필요한 수준의 연속성을 보장하기 위하여 프로세스, 절차, 통제를 수립하고 문서화하여 구현 및 유지하여야 한다.
The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

A.17.1.3 정보보호 연속성 검증, 검토, 평가
Verify, review and evaluate information security continuity
조직이 수립하고 구현한 정보보호 연속성 통제가 어려운 상황에 적절하고 효과적임을 보장하기 위하여 주기적으로 검증하여야 한다.
The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

A.17.2 이중화
Redundancies
목적: 정보처리 시설의 가용성을 보장하기 위하여
Objective: To ensure availability of information processing facilities.

A.17.2.1 정보처리 시설 가용성
Availability of information processing facilities
정보처리 시설은 가용성 요구사항을 만족하는데 충분하도록 이중화하여 구현하여야 한다.
Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

A.18 준거성
Compliance
A.18.1 법적 및 계약 요구사항 준수
Compliance with legal and contractual

requirements
목적: 정보보호에 관련된 법률, 법령, 규정, 계약 의무와 보안 요구사항의 위반을 방지하기 위하여
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

A.18.1.1 적용 법규 및 계약 요구사항 식별
Identification of applicable legislation and contractual requirements
정보시스템과 조직에 관련한 모든 법령, 규제, 계약 요구사항과 조직의 요구사항 만족을 위한 접근방법을 명시적으로 식별하고 문서화하며 최신으로 유지하여야 한다.
All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

A.18.1.2 지적재산권
Intellectual property rights
지적재산권 및 소프트웨어 제품 소유권의 행사에 관련된 법령, 규정, 계약 요구사항의 준수를 보장하기 위하여 적절한 절차를 구현하여야 한다.
Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

A.18.1.3 기록 보호
Protection of records
기록은 법령, 규정, 계약, 업무 요구사항에 따라 분실, 파손, 위조, 비인가 접근, 비인가 공개로부터 보호하여야 한다.
Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.

A.18.1.4 프라이버시 및 개인정보보호
Privacy and protection of personally identifiable information
프라이버시와 개인정보의 보호는 관련 법규와 규제에서 요구하는 바에 따르고 있음을 보장하여야 한다.
Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

A.18.1.5 암호 통제 규제
Regulation of cryptographic controls
암호 통제는 모든 관련 협약, 법규, 규제를 준수하며 사용하여야 한다.
Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

A.18.2 정보보호 검토
Information security reviews
목적: 조직의 정책과 절차에 따라 정보보호를 구현하고 운영하고 있음을 보장하기 위하여
Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

A.18.2.1 정보보호 독립적 검토
Independent review of information security
정보보호와 그 구현(예: 정보보호에 대한 통제 목적, 통제, 정책, 프로세스, 절차)에 대한 조직의 접근방법은 계획된 주기 또는 중대한 변경이 발생한 시점에 독립적으로 검토하여야 한다.
The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

A.18.2.2 보안 정책 및 표준 준수
Compliance with security policies and standards
관리자는 자신의 책임 영역 내에서 적절한 보안 정책, 표준, 기타 보안 요구사항에 대한 정보 처리 및 절차의 준거성을 주기적으로 검토하여야 한다.
Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

A.18.2.3 기술 준거성 검토
Technical compliance review
조직의 정보보호 정책 및 표준에 대한 정보시스템의 준거성을 주기적으로 검토하여야 한다.
Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

국제 정보보호 표준-ISO 27001:2013 인증 기준
(Annex A control objectives and controls)

구분	ISO 27001:2013		통제항목
통제 목적 및 통제	A.5 Information security policies	정보보호 정책	2
	A.6 organization of information security	정보보호 조직	7
	A.7 Human resource security	인적 자원 보안	6
	A.8 Asset management	자산 관리	10
	A.9 Access control	접근 통제	14
	A.10 Cryptography	암호화	2
	A.11 Physical & environmental security	물리적 환경적 보안	15
	A.12 Operations security	운영 보안	14
	A.13 Communications security	통신 보안	7
	A.14 System acquisition, development & maintenance	정보 시스템 개발 유지보수	13
	A.15 Supplier relationships	공급자 관계	5
	A.16 Information security incident management	정보보안 사고 관리	7
	A.17 Information security aspects of business continuity management	정보보호 측면 업무 연속성 관리	4
	A.18 Compliance	컴플라이언스	8
	14개 영역 통제 항목		**114 개**

작성: Reslience 메일: mssinnovator@naver.com