보안규정

제정일자	최종 수정일	개정차수
2024.03.05	2024.03.05	0

제1장 총칙

1. 목적

본 규정은 효성중공업(주) 중공업PG(이하 '회사'라 한다.)가 정보자산을 보안 위협으로부터 보호하기 위하여 필요한 업무 수행의 기본 원칙과 회사의 방침을 정하여, 모든 임직원이 준수하여야 할 정보보안 사항을 정의하는 데 그 목적이 있다.

2. 적용범위

2.1 본 규정은 회사에서 보유하는 모든 유·무형의 정보자산 및 이를 이용하는 모든 임직원, 임시 직원, 협력사, 외부인력 등을 대상으로 적용한다.

2.2 회사의 정보자산에 대한 정보보안의 실행은 본 규정을 최우선으로 하며, 규정에 명시되지 아니한 사항은 내규 또는 관련 관계 정책에서 정하는 바에 따른다.

2.3 정보보안 관련 국내의 법규 및 기준은 본 규정보다 우선하여 적용한다.

3. 용어의 정의

3.1 “정보보안”이라 함은 회사에서 발생할 수 있는 보안위험 및 사고를 회피하거나 그 영향을 최소화하여 정보자산의 기밀성, 무결성 및 가용성을 지속 유지하도록 정보자산을 보호하는 것을 말한다.

3.2 “정보자산”이라 함은 회사가 소유 및 보유하거나 회사로부터 생성된 모든 유· 무형의 경영정보, 영업정보, 고객정보, 문서(전자문서 포함), 저장매체, 정보 시스템 등 정보로써 가치를 갖는 자산과 동 자산의 가치를 유지하는 데 필요한 환경(인적, 시설, 장비 등)을 말한다.

3.3 “정보보안 관리체계”라 함은 조직의 정보자산을 체계적으로 보호하고 보안 위협으로부터 조직이 유기적으로 대응하기 위한 종합적인 관리체계를 말한다.

3.4 “정보시스템”이라 함은 정보의 수집, 가공, 저장, 검색, 송·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말하며, 서버, 네트워크, DBMS, 정보보안시스템 등이 포함된다.

3.5 “보안사고”라 함은 해킹, 악성코드 감염, DDoS 공격 등으로 정보유출, 통신망 마비, 정보시스템 파괴 등을 야기할 수 있는 사고를 의미하며, 내부자에 의한 보안사고를 포함한다.

3.6 “영상정보처리기기”라 함은 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 폐쇄회로 텔레비전 및 네트워크 카메라를 의미한다.

4. 역할과 책임

회사 정보보안에 대한 책임은 회사업무를 수행하는 모든 임직원에 있으며, 임직원은 정보보안과 관련된 기준들을 숙지하고 준수하여야 한다.

제2장 정보보안 정책 관리

본 장에서는 정보보안 정책의 대상과 목표를 정의하고 정책 체계 수립 및 제·개정 등 정보보안 정책 운영에 필요한 제반 사항을 규정하는 데 있으며, 이와 관련한 세부 사항은「정보보안 정책 운영 기준」에 따른다.

5. 정보보안 정책 수립

5.1 회사는 모든 정보자산을 안전하게 보호하고 정보보안 활동의 지속적인 운영 및 관리를 위하여 임직원이 준수하여야 할 원칙과 기준을 정의한 정보보안 정책을 수립하고 운영하여야 한다.

5.2 정보보안 정책은 '규정', '기준'으로 구성하며, 정보보안 업무를 수행하는 데 필요한 세부 기준이나 업무처리 방법 등에 대하여 회사의 업무 특성을 반영하여 '절차', '가이드' 및 '점검 체크리스트' 등 정보보안 정책 체계간 연관성이 확보될 수 있도록 구성할 수 있다.

6. 정보보안 정책 운영관리

6.1 정보보안 주관부서는 다음 각 호의 사항을 반영하여 정보보안 정책의 타당성을 정기적으로 검토하여야 하며, 정보보안 정책 제·개정 시 관련부서와의 협의가 이루어져야 하고, 이력관리를 통하여 최신으로 유지하여야 한다.

6.2 정보보안 주관부서는 정보보안 규정 및 기준을 제·개정하는 경우 정보보안 위원회의 심의를 거쳐 대표이사의 승인을 득하여야 하며, 정보보안 정책에 대한 제·개정은 회사에서 정한 승인절차를 따른다.

6.3 정보보안 주관부서는 승인을 득한 '규정'과 '기준'은 회사에 근무하는 전체 인원이 인지할 수 있도록 공표되어야 하며, 변경된 정보보안 정책을 해당 업무 담당자에게 통보 하여 관련 사항을 숙지할 수 있게 하여야 한다.

6.4 정책 문서는 회사의 사전 승인없이 외부로 일체 유출할 수 없다.

제3장 정보보안 조직 운영

본 장에서는 회사의 정보보안 정책을 수립하고 정보보안 활동이 체계적으로 수행 될 수 있도록 정보보안 전담조직을 구성하여 정보보안 활동의 실효성 및 연속성을 확보하는 데 필요한 사항을 규정하며, 이와 관련한 세부 사항은 「정보보안 조직 운영 기준」에 따른다.

7. 정보보안 전담조직 구성

7.1 회사는 조직 전반에 걸친 정보보안 활동을 체계적으로 관리 및 운영할 수 있도록 법적요건 및 업무특성을 반영하여 정보보안 조직을 구성하여야 한다.

7.2 회사는 정보보안 조직 구성 시 정보보안 업무를 총괄하는 정보보안 최고책임자를 지정하여야 하며, 정보보안 업무를 실질적으로 수행 및 운영하는 정보보안 주관부서를 구성하여야 한다.

7.3 정보보안 최고책임자는 각 부서의 정보보안 관련 이행 및 조치에 관한 정보보안 보안관련 통제를 총괄하고, 정보보안 업무를 효율적으로 수행하기 위하여 부서별 정보보안 담당자를 지정할 수 있다.

8. 정보보안 조직 운영

8.1 회사는 정보보안 주관부서를 통하여 회사 내 모든 자산을 안전하게 관리할 수 있도록 관리적, 물리적, 기술적 영역 등 정보보안 전 영역에 적용될 수 있는 정보보안 관리체계를 수립하고 운영하여야 한다.

8.2 회사는 정보보안 업무를 효율적으로 수행할 수 있도록 정보보안 주관부서의 활동을 평가할 수 있는 조직평가 체계를 수립하여야 하며, 주기적으로 정보보안 관련 활동을 평가하여야 한다.

제 4장 정보보안 위원회 운영

본 장에서는 정보보안 업무에 대한 주요사항을 심의 및 조정할 수 있도록 회사 정보보안위원회의 구성 및 역할과 운영에 관한 사항을 규정하며, 이와 관련한 세부 사항은「정보보안 위원회 운영 기준」에 따른다.

9. 정보보안 위원회 구성

9.1 회사는 정보보안 관리의 효율적인 운영 및 주요 사안에 대한 대책, 기타 보안에 관한 주요사항을 심의 및 의결하기 위하여 '정보보안 위원회'를 구성하고 운영할 수 있다.

9.2 정보보안 위원회는 조직 내 이해관계를 대변할 수 있는 정보보안 최고책임자, 정보보안 책임자, 인사, 총무, 영업, 구매, IT, 창원 관리 등 각 부서의 팀장으로 구성한다.

9.3 회사는 정보보안 위원회 의결사항에 대한 실무검토, 이행방안 수립 및 원활한 정보보안 활동의 조정을 위해 '정보보안 실무협의회'를 구성할 수 있다.

10. 정보보안 위원회 운영

10.1 '정보보안 위원회'는 정보자산의 보호 및 관리에 관한 사항 등 회사 경영에 중대한 영향을 미치는 정보보안 주요사안을 처리하기 위해 심의대상 기준을 수립하고 운영하여야 한다.

10.2 '정보보안 위원회'는 안건상정, 위원회 개최, 심의 및 의결이 정당하고 합리적으로 운영될 수 있도록 관련 절차를 마련하고 관련 기준에 따라 운영하여야 한다.

10.3 정보보안 위원회 심의 및 의결사항은 최고경영자에게 보고하여야 한다.

제5장 정보자산 보안 관리

본 장은 회사가 보유하고 있는 정보자산을 훼손, 변조, 도난, 유출 등의 다양한 침해 위협으로부터 안전하게 보호하고 체계적으로 관리하는 데 필요한 사항을 규정 하며, 이와 관련한 세부 사항은「정보자산 보안 운영 기준」에 따른다.

11. 정보자산 보안관리 원칙

11.1 회사 업무와 관련하여 직·간접적으로 생산되거나 획득한 모든 정보자산의 소유권, 기타 지적재산권 등의 제반권리는 회사에 있다.

11.2 정보자산의 안전한 관리를 위하여 정보자산의 도입 및 생성부터 폐기 까지의 관리기준을 수립, 운영하여야 한다.

11.3 회사는 산업기밀, 영업비밀 관련 정보자산 등은 해당 법령에 준하여 보안대책을 수립 및 운영하여야 한다.

12. 정보자산 식별 및 평가

12.1 회사는 정보자산에 대한 적절한 관리와 통제를 위하여 정보자산별 특성에 따라 정보자산 분류기준을 수립하고 정보보안 관리체계 범위 내 모든 정보자산을 식별하여야 한다.

12.2 회사는 식별된 정보자산에 대하여 정보자산의 유출, 장애 및 침해 발생 시 조직의 업무에 미치는 잠재적 영향과 손실을 고려하여 정보자산의 가치를 평가 할 수 있도록 측정 기준을 수립하고 운영하여야 한다.

13. 위험분석 및 평가

13.1 회사는 자산의 중요도와 기밀성·무결성·가용성 측면에서의 위협·취약성 수준에 따라 정보자산별 위험을 파악하고 관련 위험이 지속적으로 감소될 수 있도록 조직에 적합한 위험분석 및 평가방안을 수립하고 운영하여야 한다.

13.2 회사는 식별된 위험에 대한 영향도 및 수준을 파악하여 잠재적 위험이 최소화될 수 있도록 적절한 보호대책을 수립하여 지속적으로 위험관리를 수행하여야 한다.

제6장 인적 보안 관리

본 장은 임직원의 채용, 직무변경, 퇴직 등 인사 업무 수행 시 필요한 보안 관련 법·제도적 사항을 준수하고, 인적요인에 의하여 발생할 수 있는 다양한 보안 위협을 예방하는 데 필요한 사항을 규정하며, 이와 관련한 세부 사항은「인적 보안 운영 기준」에 따른다.

14. 인적 보안관리 기준

14.1 회사는 인사 업무상 발생될 수 있는 보안 위협을 최소화하기 위하여 임직원의 인사 업무 수행과 관련한 보안관리 및 통제 대책을 수립하여야 한다.

14.2 회사는 주요 직무에 대한 체계적인 관리 및 권한 오남용을 예방하기 위하여 주요 직무자를 지정하고, 직무 분리 기준을 수립하여 운영하여야 한다.

14.3 회사는 임직원의 역할과 책임을 명확하게 하기 위하여 업무 목적에 따른 '정보보안 서약서'를 상시 또는 정기적으로 징구하여야 하며, 위반자에 대한 공식적인 처리 절차를 수립하여야 한다.

15. 정보보안 의식제고

15.1 회사는 임직원의 정보보안 인식제고 및 보안사고 예방을 위하여 보안 수칙 준수에 필요한 정보보안 교육을 상시 또는 정기적으로 실시하여야 한다.

15.2 회사는 정보보안 교육의 효과적인 개선을 위하여 교육 완료 후 교육에 대한 평가를 실시하여 차기 교육 계획에 반영하여야 한다.

제7장 외부인력 보안 관리

본 장에서는 회사와 계약관계에 있는 외부업체 및 외부인력에 대해 계약에서부터 종료까지 발생할 수 있는 정보유출, 변조, 오남용 등의 보안위협을 최소화하는 데 필요한 사항을 정의하며, 관련 세부 사항은「외부인력 보안 운영 기준」에 따른다.

16. 외부인력 관리 기준

16.1 회사는 외부인력에 의하여 발생할 수 있는 정보보안 위협을 최소화하기 위하여 외부업체 및 외부인력에 대한 관련 정책을 수립하고 운영하여야 한다.

16.2 회사는 외부업체 계약 및 외부인력 투입 시 각 단계별 보안요건을 수립하여 운영 하여야 한다.

17. 외부인력 보안 운영

17.1 회사는 외부인력을 대상으로 보안정책 및 업무상 필요한 보안 준수사항에 대하여 교육을 수행하고, 주기적으로 보안준수 여부를 점검하여야 한다.

17.2 회사는 외부인력이 비밀유지, 보안준수 의무, 위반 시 책임 등 보안 요건을 준수하도록, 정보보호 서약서 징구 등의 의무사항을 이행하도록 하여야 한다.

제8장 임직원 보안 관리

본 장은 모든 임직원이 회사의 자산을 안전하게 보호하고 효율적으로 이용 및 관리하기 위하여 정보보안 관련 의무와 책임을 정의하는 데 필요한 사항을 규정 하며, 이와 관련한 세부 사항은「임직원 보안 운영 기준」에 따른다.

18. 임직원 보안관리 기준

18.1 회사는 모든 임직원이 준수하여야 할 의무와 책임을 명확하게 하기 위하여 임직원 보안관리 기준을 수립하여야 한다.

18.2 회사는 임직원 보안 기준의 변경 시 교육 또는 공지를 통해 임직원이 인지할 수 있도록 하여야 한다.

19. 임직원 보안 운영

19.1 회사의 모든 임직원은 관련 정책에 명시되어 있는 정보보안 의무사항을 준수 하여 업무를 수행하여야 한다.

19.2 회사는 관련 정보보안 정책에 대한 임직원의 준수여부를 상시 또는 정기적으로 점검 하여야 한다.

제9장 정보시스템 운영 보안

본 장은 정보자산의 유출 및 파괴, 불법적인 행위 등으로 인한 보안사고로부터 정보시스템을 안전하게 보호하기 위하여 보안업무 운영기준을 수립하는 데 필요한 사항을 규정하며, 이와 관련한 세부 사항은「정보시스템 운영보안 기준」에 따른다.

20.정보시스템 운영보안 기준

20.1 회사는 최적의 정보시스템 운영환경을 구축하고 지속적으로 서비스를 제공하기 위하여 정보시스템 운영보안 기준을 수립 및 운영하여야 한다.

20.2 회사는 정보시스템 자산에 대한 운영보안 기준이 정상 가동될 수 있도록 보안성 검토 등을 통하여 정기적으로 점검하여야 한다.

20.3 개인정보취급 및 영업비밀 등 관련 정보자산은 해당 법령에 적합한 보안대책을 수립 및 운영하여야 한다.

21. 정보시스템별 통제 기준

21.1 회사는 보유 자산을 외부의 위협으로부터 안전하게 보호하기 위하여 정보시스템 제반 환경에 대한 관리적, 물리적, 기술적 보호대책을 수립하여야 한다.

21.2 회사는 비 인가자에 대한 정보시스템 자원 접근을 차단하고, 정당한 사용자가 허가되지 않은 방법으로 자원에 접근하는 것을 제한하여야 한다.

제10장 어플리케이션 보안 관리

본 장은 회사의 어플리케이션이 안전하게 개발 및 운영될 수 있도록 보안 관련 사항을 정의하고, 어플리케이션을 안정적으로 관리 및 운영하는 데 필요한 사항을 규정하며, 이와 관련한 세부 사항은「어플리케이션 보안 운영 기준」에 따른다.

22. 어플리케이션 개발보안

22.1 회사는 어플리케이션을 안전하게 개발하기 위하여 어플리케이션 기획 및 분석, 설계, 개발, 테스트 및 이관 등 각 개발 단계에 필요한 보안기준과 절차를 수립 하고 운영하여야 한다.

22.2 회사는 개발 및 테스트시스템에 대하여 물리적으로 운영시스템과 분리하고, 개발 및 테스트시스템의 보안관리는 운영시스템의 수준으로 관리하여야 한다.

23. 어플리케이션 운영 및 변경관리

23.1 회사는 개발이 완료되어 운영환경으로 이관된 어플리케이션에 대하여 별도의 보안운영 기준을 수립 및 운영하여, 어플리케이션이 안전하게 운영될 수 있도록 관리·감독하여야 한다.

23.2 회사는 어플리케이션의 개선을 위하여 변경작업이 필요한 경우 기존 시스템 보안 위배 여부를 고려하여 변경작업에 관한 절차를 마련하여 수행하여야 한다.

제11장 원격근무 보안 관리

본 장은 회사 외부에서 원격으로 회사 업무 수행 및 내부 관련 시스템에 접속하는 방식의 업무 수행 시의 회사 정보자산을 안전하게 보호하는 데 필요한 사항을 규정하며, 이와 관련한 세부 사항은 「원격근무 보안 운영 기준」에 따른다.

24. 원격근무 보안 운영 기준

24.1 회사는 외부 공간에서 회사 업무를 수행하는 비대면 업무 방식인 원격근무 환경 에 대한 보안운영 기준을

수립 및 운영하여야 한다.

24.2 회사는 원격근무 시 정보자산 보호 및 관리를 위한 계정 및 접근권한, 인증 등 관리적·기술적 보호대책을 수립 및 운영하여야 한다.

25. 원격근무 통제 기준

25.1 회사는 원격접속을 이용하는 모든 사용자가 관련 정책을 숙지하도록 안내하고 사용자는 정보보안 의무사항을 준수하여 업무를 수행하여야 한다.

25.2 회사는 관련 원격접속에 따른 보안사고 예방 및 대응을 위한 방안을 수립 및 운영하여야 한다.

제12장 보안사고 대응 관리

본 장은 보안사고 징후 인지 및 보안사고 발생 시 신속한 조치를 통하여 피해를 최소화하고, 보안사고에 효과적으로 대응하는 데 필요한 사항을 규정하며, 이와 관련한 세부 사항은「보안사고 대응 운영 기준」에 따른다.

26. 보안사고 대응체계 수립 및 운영

26.1 회사는 내·외부의 위협으로 인한 보안사고 발생 시 사고 유형에 따라 신속하게 대응 및 조치할 수 있도록 보안사고 대응체계를 마련하여 운영하여야 한다.

26.2 회사는 보안사고 징후 인지 및 보안사고 발생 시 보안사고 대응체계에 따라 신속하게 조치하고 보고체계에 따라 내부 또는 감독기관에 보고하여야 한다.

26.3 회사는 보안사고 발생 시 원인을 분석하여 피해확산을 방지하고 보안사고 정보를 실시간으로 수집·탐지 및 분석·대응·전파할 수 있도록 외부기관과 연계 등의 조치를 취하여야 한다.

27. 보안사고 예방 및 재발방지

27.1 회사는 보안사고의 재발방지를 위한 추가 조치 필요성을 확인한 후 재발방지 대책을 수립하고, 보안사고를 예방하기 위해 정기적으로 점검하여야 한다.

27.2 회사는 보안사고를 예방하기 위하여 정기적으로 보안사고 대응 방안 검토 및 교육을 실시하고, 개선 사항에 대하여 지속적으로 조치하여야 한다.

제13장 물리적 보안 관리

본 장은 사무실, 전산실 등 회사의 주요 시설 및 장소를 안전하게 보호하기 위한 물리적 보안 기준을 명시함으로써 훼손, 도난, 변조, 유출 등 다양한 형태의 침해 위협을 최소화하고 정보자산을 보호하는 데 필요한 사항을 규정하며, 이와 관련한 세부 사항은「물리적 보안 운영 기준」에 따른다.

28. 출입 통제 관리

28.1 회사는 업무의 중요도 및 정보자산 위치에 따라 물리적 보안구역을 구분하고, 보안상 출입통제가 요구되는 구역을 보안구역으로 지정하여야 한다.

28.2 회사는 보안구역에 대한 비인가자의 출입을 방지하기 위하여 보안구역별 통제 대책을 수립 및 이행하여야 한다.

28.3 회사는 정보유출을 예방하기 위하여 공식적인 출입통제 절차 및 정보자산 반·출입 통제 기준 등 임직원 및 정보자산에 대한 출입통제 기준을 수립 및 이행하여야 한다.

29. 전산장비 및 시설 관리

29.1 회사는 전산장비 및 정보시스템을 환경적 또는 물리적 위협으로부터 보호하고, 고장, 장애 등에 의한 서비스 중단 사태가 발생하지 않도록 주기적으로 유지·관리하여야 한다.

29.2 회사는 시설에 대한 보안통제가 정상 운영될 수 있도록 문서고, CCTV, 사옥, 통신 등의 보안관리대책을 수립 및 이행하여야 한다.

제14장 개인정보 보호 관리

본 장은 회사에서 수집되는 개인정보의 보호를 위한 대책을 수립하여 불법 유출, 훼손 등으로 인한 법/제도적 준거성 확보에 필요한 사항을 규정하며, 이와 관련한 세부 사항은「개인정보 보호 운영 기준」에 따른다.

30. 개인정보 보호 조직구성

30.1 회사는 조직 전반에 걸친 개인 정보보호 활동을 체계적으로 관리 및 운영할 수 있도록 법적요건 및 업무특성 등을 반영하여 개인정보 보호책임자를 지정하여 운영하여야 한다.

30.2 개인정보 보호책임자는 법적요건 등에서 명시하고 있는 관련 업무에 대해 회사 내 개인정보 기준이 적용 및 이행되도록 총괄하고 개인정보 보호 제반 활동 전반에 걸쳐 관리·감독을 수행하여야 한다.

31. 개인정보의 보호조치

31.1 회사는 개인정보의 안전한 취급과 관리를 위하여 개인정보의 수집부터 파기까지 개인정보 생명주기에 기반한 개인정보 보호조치를 수행해야 하며, 개인정보 유출 등의 사고 발생 시 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

31.2 회사는 이용자의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 보안대책을 마련 하여야 하며, 이와 관련한 세부 사항은「개인정보 내부관리계획 운영 기준」에 따른다.

31.3 회사는 영상정보처리기기를 설치·운영 시 관련 법률에서 요구하는 설치 근거, 설치목적, 촬영범위, 책임자 지정, 영상정보의 촬영시간, 영상정보처리기기 설치 및 관리 등의 위탁에 관한 사항 등 관련 기준을 수립하여 운영하여야 하며, 이와 관련한 세부 사항은「영상정보처리기기 설치 및 운영 기준」에 따른다.

제15장 준거성 관리

본 장에서는 임직원이 준수하여야 하는 정보보안 관련 법규 및 내부 규정에 대한 직원의 준수 여부를 점검하는 데 필요한 제반 사항을 규정한다.

32. 법적 요구사항 준수

32.1 회사 정보보안 주관부서는 관련부서와 협조하여 회사의 업종에 따라 관련 정보보안 법령의 요구사항을 식별하고, 법적 요구사항 준수를 위하여 적합한 내부통제 기준을 수립하고 운영하여야 한다.

32.2 정보보안 관련 법령 및 기준의 적용 범위는 회사에 소속된 임직원 및 계약에 따른 외부인력을 포함하고, 회사를 방문하는 모든 외부인을 대상으로 한다.

32.3 회사는 법률에 근거하여 외부기관에 보고가 필요한 각종 정보보안 관련 문서 작성 시 관련부서의 사전 검토를 거쳐야 한다.

32.4 본 규정 시행에 있어 영업 및 업무상 필요하다고 인정되는 경우나 해당 사안에 따라 담당 팀장 또는 정보보안 주관부서 팀장의 승인이 있는 경우 예외사항을 적용할 수 있다.

33. 포상 및 징계

33.1 회사 정보보안 주관부서는 임직원 및 외부인력의 정보보안 정책 준수 여부를 관리하여 해당 사항에 대한 포상 및 징계가 이루어질 수 있도록 기준을 수립하고 운영하여야 한다.

33.2 회사는 임직원이 본 규정을 위반하여 정보보안에 부정적인 영향을 끼치는 경우 관련 규정에 따라 처리하며 필요 시 법적수단에 따른 처벌을 강구할 수 있다.

33.3 회사는 계약관계에 있는 외부인력의 정보보안 정책 위반 시 사업장 출입을 제한 할 수 있으며, 위반사실을 외부업체에 통보하여야 한다. 또한 중대한 위반 발생 시 계약파기, 손해배상 등의 필요조치를 수행할 수 있다.

제16장 실행방안 및 목표

34. 실천지침 및 중장기 목표

34.1 회사 및 임직원은 기밀 정보를 책임있게 관리하기 위해 노력한다.

34.2 기업의 정보 자산 보안을 관리하여 국가 기술 정보 자산 관리에 기여한다.

34.3 2025년 정보유출 사건을 Zero화 한다.

34.4 2030년까지 정보 및 개인정보 보호 관련 주제 교육을 임직원 100%가 수강하도록 한다.