정보보호정책

감사팀

2023. 12. 4.

개정 이력

NO	Ver[1]	작성일	구분[2]	개정 사유 및 내용[3]	작성자[4]	승인자
1	0.1	2023.12.4.	신규	최초작성	가예람	이용운

목 차

문서번호	TYM 보안-01	정보보호정책	개정차수	1
문서버전	V0.1		개정일자	2023.12.4.

제 1 장 총칙

제 1 조(목적)

본 정책은 ㈜티와이엠(이하 '회사'라 한다)의 정보보호 활동을 위해 필요한 사항을 규정하여 회사의 정보자산을 보호함을 목적으로 하며, 모든 구성원은 본 정보보호 정책을 준수하여야 한다.

제 2 조(적용범위)

본 정책은 회사에 근무하는 전 구성원과 외부인력, 출입자 등을 대상으로 적용되며, 본 정책에서 정한 범위 내에서 직·간접적인 관계에 있는 회사 및 계약관계에 있는 모든 인력에게 적용된다. 또한, 정보보호의 적용범위는 회사의 정보자산으로 한다.

제 3 조(용어정의)

본 정책에 사용하는 용어의 정의는 다음과 같다.

① "정보"란 재무정보, 경영정보, 개인정보, 영업정보, 기술정보 등 회사와 관련된 모든 정보를 말한다.

② "정보자산"이란 제 1 호에서 정의한 정보의 가치를 지닌 자료, 문서, 소프트웨어, 하드웨어 및 정보 그 자체를 나타내는 유·무형의 모든 자산을 말한다.

③ "정보보호"란 정보의 수집, 가공, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하고 수행하는 것을 말한다.

④ "정보보호 최고책임자"란 회사의 정보보호를 위한 관리적·기술적 수단의 마련 및 활동 수행을 총괄 관리할 수 있는 임원을 말한다.

⑤ "개인정보"란 주민등록번호 등 특정 개인을 식별할 수 있는 정보와 서비스 이용 기록, 구매내역 등 서비스를 이용하는 과정에서 생성되는 정보, 그리고 다른 정보와 용이하게 결합하여 개인 식별이 가능한 정보 등 특정 개인과 관련된 모든 정보를 말한다.

⑥ "개인정보 보호책임자"란 회사 내에서 개인정보를 취급하는 특정 사업을 주관하는 임원이나 개인정보와 관련된 이용자의 고충처리를 담당하는 부서의 장을 말한다.

⑦ "개인정보 취급자"란 개인정보처리시스템의 접근/접속 권한을 보유하고 있거나, 업무상 또는 서비스 제공을 위해 개인정보를 취급(수집, 보관, 이용, 처리, 제공, 관리, 파기 등)하는 회사 및 외부업체 직원을 말한다.

⑧ "비밀번호"란 이용자 및 개인정보 취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수

있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

⑨ "보조저장매체"란 외장 HDD, USB 메모리, 플래쉬메모리, CD/DVD, PMP, MP3 등 휴대가 용이하고 정보의 저장이 가능한 모든 매체를 말한다.

⑩ "구성원"이란 회사의 정보자산을 관리, 운영, 활용하는 임직원 및 계약직원(계약직, 임시직, 아르바이트 등)을 말한다.

⑪ "외부업체"란 회사와 계약을 통해 업무의 일부를 위탁 받거나 회사에 용역을 제공하는 법인으로서, 업무상 회사 정보시스템에 접속하거나 회사의 정보 및 개인정보 취급하는 법인을 말한다.

⑫ "외부인력"이란 회사와 계약 또는 제휴를 맺은 외부업체 소속 직원과 외부업체와 계약에 의해 위탁 또는 제휴 업무를 수행하는 모든 인력을 말한다.

⑬ "정보시스템"이란 정보를 처리, 저장, 전달할 목적으로 회사가 사용 또는 관리하는 모든 PC, 서버, 네트워크, 보안장비 등 하드웨어와 그 하드웨어에 포함된 데이터베이스, 어플리케이션 등 소프트웨어를 말한다.

⑭ "침해사고"란 회사가 제공하는 모든 서비스가 해킹 또는 악성코드 등에 의해 지연·파괴되거나, 회사의 기업비밀 및 개인정보가 무단 노출/유출되는 것을 말한다.

⑮ "업무용 PC"란 원활한 업무 수행을 위해 회사가 임직원에게 지급한 PC 를 말한다.

제 2 장 정보보호 정책 및 지침

제 4 조(정책 및 지침의 제·개정)

① 정보보호 최고책임자는 정보보호 정책 및 그 시행을 위해 필요한 절차, 시기, 방법 등을 구체적으로 정한 지침을 수립하여야 한다.

② 정보보호 정책 및 지침은 법적 준거성, 업무 영향도 등을 고려하여 제·개정할 수 있다.

제 5 조(정책 및 지침의 유지관리)

① 정보보호 최고책임자는 정보보호 정책 및 지침에 대해 연 1 회 이상 다음 각 호의 사항을 포함한 타당성 검토를 수행하고 필요 시 관련 정책 및 지침을 제·개정하여야 한다.

1. 상위조직 및 관련기관의 정보보호 정책과의 연계성 및 적정성
2. 정보보호 정책 및 지침의 일관성
3. 정보보호 관련 법령의 제·개정사항 및 법적 준거성 반영
4. 위험평가 및 관리체계 점검 결과 반영

5. 회사의 대내외 환경 변화 등

② 정보보호 정책 및 지침을 제·개정할 경우에는 이해 관계자의 검토를 받고 검토사항을 기록하여야 한다.

③ 정보보호 정책 및 지침의 제·개정 이력을 관리하여야 한다.

제 6 조(정책 및 지침의 공표)

① 정보보호 정책 및 지침은 이해 관계자가 쉽게 접근할 수 있도록 최신 형태로 제공되어야 한다.

② 제 1 항에도 불구하고 정보보호 지침에서 정한 절차, 서식, 별첨 자료는 이해 관계자를 제외하고 공개를 제한할 수 있다.

제 3 장 정보보호 조직의 운영

제 7 조(정보보호 조직 구성)

① 정보보호 최고책임자는 다음 각 호의 업무를 수행하기 위하여 정보보호관리자, 시스템관리자를 지정하여 운영할 수 있다.

1. 정보보호 정책 및 지침의 수립 및 이행
2. 정보보호 조직의 구성 및 운영
3. 정보보호 자원(예산 및 인력) 지원 및 조정
4. 정보보호 교육 계획 수립 및 실시
5. 정보보호 관리체계 구축 및 운영 총괄 관리(위험평가, 보호대책 이행, 관리체계 점검 등

② 정보보호관리자는 회사의 정보보호 주관부서의 관리자로서 정보보호 관련 각종 계획 수립 및 정보보호 업무에 대한 조정, 통제, 필요한 업무를 관리·감독하며, 정보보호 책임자를 보좌하여 정보보호 관련 업무를 수행한다.

③ 정보보호담당자는 정보보호 조직 구성원이며 회사 내 정보보호 계획에 따른 활동을 수행하여야 한다.

④ 시스템관리자는 서버, 네트워크, 데이터베이스 등 업무분야를 관리하고 있는 각 담당자로서 정보시스템을 안정적으로 운영하여야 하며, 중요한 데이터의 적절한 관리기준 및 절차를 수립 및 시행하여야 한다.

제 8 조(정보보호위원회 운영)

① 회사의 전반에 걸친 중요한 정보보호 관련사항에 대해 검토 및 의사결정을 할 수 있는 정보보호위원회를 구성하여야 한다.

② 정보보호위원회의 위원은 정보보호 최고책임자로 하며, 관련사업 부문, 본부의 간부급으로 구성한다.

③ 정보보호위원회는 조직 전체의 정보보호 목표, 목적 및 우선순위 등을 고려하여 회사의 정보보호 주요 현안을 검토하고 이에 대한 의사결정을 수행한다.

제 4 장 인력 보안 관리

제 9 조(정보보호 서약 및 갱신)

① 구성원은 입사 및 퇴사 시 회사의 정보보호 정책을 이해하고, 이를 준수하겠다는 내용의 정보보호 서약서를 제출해야 하며, 연 1 회 주기적으로 갱신하여야 한다.

② 구성원의 퇴사 시 정보보호 서약서를 징구하고, 보유중인 회사의 모든 정보자산 및 정보시스템 사용권한, 사원증 등을 회수하여 개인 물품 이외의 반출이 불가하도록 하여야 한다.

③ 정보보호 서약과 관련된 구체적인 사항은 'TYM 보안-03.인적보안지침'을 참조한다.

제 10 조(정보보호 교육)

① 정보보호관리자는 교육 대상, 교육방법 및 내용, 교육 일정, 횟수 등을 포함하여 연간 정보보호 교육 및 훈련 계획을 수립하여야 한다.

② 회사의 구성원 등을 대상으로 정보보호 정책 및 업무상 필요한 정보보호 활동을 교육하고 홍보함으로써 구성원의 정보보호 인식을 제고하는 데 그 목적이 있다.

③ 정보보호 교육 및 훈련은 전 구성원을 대상으로 연 1 회 이상 정기적으로 실시하여야 한다.

④ 정보보호 교육은 구성원 등이 회사의 정보보호 활동을 이해하고 수행할 수 있도록 업무 및 수준 등을 고려하여 이행하여야 한다.

⑤ 정보보호 교육을 수행하는데 있어 내부 교육, 외부 위탁교육 등 다양한 방법을 활용할 수 있다.

⑥ 정보보호관리자는 정보보호 교육 이행 후 평가를 실시하여 교육의 효과 및 문제점을 분석하고, 추후 정보보호 교육 계획에 반영해야 한다.

제 5 장 외부인력 보안 관리

제 11 조(계약 시 보안 요구사항)

① 외부인력 또는 외부업체와 계약을 할 경우, 비밀유지, 정보보호 준수 의무, 정보보호 문제 발생 시의 손해배상 책임 등 정보보호 요건을 정의하여 계약서 상에 반드시 반영해야 하며, 필요 시 별도의 정보보호 약정서를 징구할 수 있다.

② 정보보호관리자는 계약서 및 정보보호 약정서에 명시된 보안 요구사항의 이행여부를 관리·감독하여야 한다.

③ 외부업체 계약과 관련된 구체적인 사항은 'TYM 보안-03.인적보안지침'을 참조한다.

제 12 조(업무 수행 시 보안 요구사항)

① 외부인력의 업무 수행 시 회사의 보안 정책 및 업무상 필요한 정보보호 활동에 대해 교육 후 보안 정책의 준수와 비밀유지에 대한 정보보호 서약서를 징구하여야 한다.

② 외부인력의 보안 관리 정책 위반 시 그 결과에 대해 해당 업체에 경고 조치하고, 계약에 따른 해지, 손해배상 등의 필요 조치를 수행하여야 한다

제 13 조(계약 종료 시 보안 요구사항)

① 외부인력의 계약 종료 시 정보보호 서약서를 징구하며 보유 중인 회사의 모든 정보자산 및 정보 시스템 사용 권한, 출입 권한 등을 회수 및 파기하여 개인 물품 이외의 반출이 불가하도록 하여야 한다.

제 6 장 정보자산의 보안관리

제 14 조(정보자산 등급 분류 및 관리)

① 정보보호관리자는 회사의 정보자산에 대한 중요도를 평가하여 보안 등급별로 분류기준을 수립하고 정기적으로 적정성을 검토하여야 한다.

② 정보자산은 보안 등급에 따라 취급절차(생성, 저장, 이용, 파기 등) 수립 및 사용자를 지정하고 비 인가자의 접근을 차단하여야 한다.

③ 중요 데이터 및 문서 등의 폐기 시에는 해당 내용을 복구할 수 없도록 파기 또는 완전 삭제 등을 시행하여야 한다.

④ 정보자산과 관련한 구체적인 사항은 'TYM 보안-02.정보자산관리지침'을 참조한다.

제 15 조(정보자산의 위험관리)

① 정보보호관리자는 정보자산의 중요도, 취약 정도, 위협 정도를 기반으로 위험도를 평가하고 위험 관리 계획을 수립하여 관리하여야 한다.

② 정보보호관리자는 위험 관리 계획에 따른 보호 대책을 수립할 경우에는 긴급성(위험 수준), 소요되는 자원(예산, 인력), 구현 가능성(기대 효과) 등을 고려하여 우선순위를 결정한다.

제 7 장 개인정보보호

제 16 조(내부관리계획의 수립 및 공표)

① 개인정보 보호책임자는 개인정보 보호와 관련한 법령 및 정책 등을 준수할 수 있도록 내부관리 계획을 수립하고 관련 법령의 제·개정 사항 등을 반영하기 위하여 연 1 회 이상 내부관리 지침의 타당성과 개정 필요성을 검토하여야 한다.

② 개인정보 보호책임자는 연 1 회 이상으로 내부관리 지침의 이행 실태를 점검·관리하고 그 결과에 따라 적절한 조치를 취하여야 한다.

③ 개인정보 보호책임자는 승인된 개인정보 내부관리 지침을 모든 구성원 및 관련자에게 알림으로써 이를 준수하도록 하고 구성원이 언제든지 열람할 수 있는 방법으로 비치하거나 제공하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제 17 조(개인정보보호조직 역할 및 책임)

① 회사는 개인정보 보호책임자를 지정하고, 다음의 업무를 총괄하여 지휘·감독한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 기타 개인정보보호 법령상 규정하는 업무

② 개인정보 보호관리자는 회사의 개인정보 주관부서의 관리자로서 개인정보보호 관련 각종 계획 수립 및 개인정보보호 업무에 대한 조정, 통제, 필요한 업무를 관리·감독하며, 개인정보 보호책임자를 보좌하여 개인정보보호 관련 업무를 수행한다.

③ 개인정보 보호담당자는 개인정보보호 조직 구성원이며 회사 내 개인정보보호 계획에 따른 활동을 수행하여야 한다.

④ 개인정보 취급자는 개인정보를 처리하는 업무를 담당하는 자(구성원, 파견근로자, 시간제 근로자 포함)로 개인정보를 처리함에 있어 동 계획은 물론, 개인정보 보호와 관련한 법령 및 정책 등을 준수하여야 한다.

제 18 조(개인정보보호교육)

① 개인정보 보호책임자는 개인정보취급자를 대상으로 개인정보보호교육 계획을 수립하고 실시하여야 한다.

② 개인정보보호교육과 관련한 구체적인 사항은 'TYM 보안-08.개인정보내부관리계획'을 참조한다.

제 19 조(개인정보의 기술적·관리적·물리적 보호조치)

① 개인정보 보호책임자는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하며, 내·외부자의 불법적인 접근 및 정보보안사고 방지를 위해 고유식별정보, 비밀번호 등 암호화, 접근통제, 악성프로그램 등 방지를 위한 보호조치를 하여야 한다.

② 개인정보 보호책임자는 개인정보의 안전한 처리를 위하여 개인정보 보호책임자 지정, 개인정보 유출사고 대응체계 수립, 개인정보의 위험도 분석 및 대응, 개인정보의 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독 등의 보호조치를 하여야 한다.

③ 개인정보 보호책임자는 전산실, 자료보관실, 문서고 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 두고 있는 경우 출입통제 절차 수립·운영 등 보호조치를 하여야 한다

④ 개인정보의 기술적·관리적·물리적 보호조치와 관련한 구체적인 사항은 'TYM 보안-08.개인정보내부관리계획'을 참조한다.

제 8 장 정보기기 보안 관리

제 20 조(정보기기 보안 관리)

① 회사에서 지급한 업무용 PC 는 본래 사용 목적 외의 용도로 사용하지 않아야 하며, 회사의 보안정책을 준수하여 사용 및 관리하여야 한다.

② 정보보호관리자는 업무용 PC 의 관리 부주의에 따른 보안 사고가 발생하지 않도록 보호 대책을 수립하여 관리하여야 한다.

③ 업무용으로 개인 보조저장매체를 사용하지 않아야 하며, 부득이하게 사용해야 할 경우 사용 허가된 매체만 사용할 수 있도록 한다.

제 9 장 정보시스템 보안 관리

제 21 조(접근권한 부여 기준)

① 모든 접근권한은 허용된 자에 한하여 업무수행에 필요한 최소한의 범위로 부여하여야 한다.

② 시스템 사용자 계정 발급 시 사용자별 한 개의 계정을 발급하여야 한다.

③ 접근권한을 부여받은 이용자는 접근권한을 임의로 양도, 대여해서는 안 되며, 책임자는 이를 수시로 확인하여야 한다.

제 22 조(비밀번호 관리)

① 정보시스템은 다음 각 호의 사항을 포함한 사용자 비밀번호 작성규칙을 적용하여야 한다.

1. 영문자·숫자·특수문자 조합규칙 적용

가) 2 종류 이상 조합 최소 10 자리 이상 또는

나) 3 종류 이상 조합 최소 8 자리 이상

2. 비밀번호 변경주기를 분기별 1 회 이상으로 설정
3. 연속적인 숫자, 생일, 전화번호 등 추측하기 쉬운 비밀번호 설정 제한 권고

② 정보시스템의 비밀번호는 다음의 각 호의 사항을 포함하여 관리하여야 한다.

1. 정보시스템 도입 시 설정된 초기 또는 임시 비밀번호 변경
2. 비밀번호 입력 또는 변경 시 마스킹 처리 적용
3. 비밀번호 저장 시 일방향 암호화 적용
4. 침해사고 등 비밀번호 노출 징후가 의심되는 경우 즉시 비밀번호 변경

③ 정보시스템 사용자는 제 3 자에게 본인의 계정 및 비밀번호를 제공해서는 아니 되며, 계정 및 비밀번호의 사용과 관련한 보안 책임은 사용자 본인에게 있다

제 23 조(계정 및 권한 관리)

① 사용자 계정을 발급·변경·해지하거나 접근권한을 부여·변경·말소하는 경우 정보시스템 계정 발급 신청을 통해 처리하여야 하며 사용자 계정 및 접근권한에 대한 관리 내역은 책임추적성을 확보할 수 있도록 정보시스템에 전자적으로 기록하고, 그 이력을 최소 3 년간 보관하여야 한다.

② 계정 및 권한 관리와 관련한 구체적인 사항은 'TYM 보안-05.정보시스템운영보안지침'을 참조한다.

제 24 조(서버 보안 관리)

① 서버를 도입할 경우에는 보안성에 대한 검토를 실시하여야 하고, 적절한 보안설정을 적용하여야 한다.

② 서버의 보안성 확보를 위해 OS 및 소프트웨어의 주요한 패치를 지속적으로 적용하여야 하며, 패치는 반드시 사전 테스트를 통해 보안패치의 안전성을 검증 후 적용하여야 한다.

제 25 조(네트워크 보안 관리)

① 업무의 특성 및 중요도에 따라 네트워크 영역을 분리하고, 분리된 네트워크 영역 간에는 접근통제를 수행하여야 한다.

② 네트워크 이용에 대한 접근 규칙 및 보안성 검토 등을 통한 점검 및 보호대책을 수립하고 적용해야 한다.

제 26 조(데이터베이스 보안 관리)

① 데이터베이스는 무결성 확보를 위하여 사용자가 직접 접근할 수 없도록 통제하여야 한다

② 데이터베이스의 접근권한은 사용자의 직무별로 구분하여 부여하고, 특정 명령(Update, Delete 등)은 권한이 부여된 자만이 사용 가능 하도록 통제하여야 한다.

제 27 조(정보보호시스템 보안 관리)

① 네트워크를 통한 침입을 방지하기 위한 기술적 수단으로써 방화벽, 침입차단시스템, 가상사설망 등의 정보보호시스템을 설치·운영하여야 한다.

② 정보보호시스템의 보안정책이 변경되어야 하는 경우 반드시 시스템관리자의 승인을 득한 후 수행해야 하며, 관련 내역을 반드시 기록·관리하여야 한다.

제 10 장 암호화

제 28 조(암호화 기준)

① 다음 각 호의 해당하는 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

② 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 고유식별정보를 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 저장하는 경우 반드시 암호화하여야 한다.

④ 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.

⑤ 안전한 암호화 알고리즘의 범위는 한국인터넷진흥원의 검증대상 암호알고리즘으로 한정한다.

제 11 장 물리 보안 관리

제 29 조(보호구역 지정)

① 중요 정보자산을 보호하기 위한 물리적 보호구역을 접견구역, 제한구역, 통제구역으로 구분하여 지정한다.

제 30 조(보호구역 분류 기준)

① 접견구역은 외부자의 출입이 가능한 장소를 말한다.

② 제한구역은 출입이 허가된 자만 출입이 가능한 장소를 말한다.

③ 통제구역은 추가적인 출입 통제 절차 및 방법이 요구되는 제한구역을 말한다.

④ 보호구역 분류 기준과 관련된 구체적인 사항은 'TYM 보안-04.물리보안지침'을 참조한다.

제 31 조(통제구역)

① 통제구역은 각종 재해에 대비하여 필요한 보호설비를 갖추고 운영절차를 수립 및 운영하여야 한다.

② 통제구역은 출입 인가자만 출입하도록 출입통제시스템 등을 설치하고 출입기록에 대해 1 년 이상 보관하여야 한다.

③ 통제구역과 관련된 구체적인 사항은 'TYM 보안-04.물리보안지침'을 참조한다.

제 12 장 정보보안 점검 및 감사

회사의 정보보호 점검, 취약점 점검, 물리 보안 등 보안관리 규정에서 정의하는 관리 대상에 대한 정보보호 이행 점검의 세부 사항을 정하는데 그 목적이 있다.

제 32 조(정보보안 점검 영역)

① 정보보안 점검은 그룹 보안 Framework 기반, 정보보호 관리체계(ISMS) 등 다음 각 호에 대한 이행 여부를 점검한다.

1. 그룹 보안 Framework 기반 점검
2. 정보보호 관리체계(ISMS) 자체 점검

3. 상시 모니터링 (정보 유출, 보안 지침 위반 등)
4. 정보보호의 날 운영
5. 생활 보안 점검
6. 정보시스템 취약점 점검
7. 기타 정보보호 및 개인정보보호 컴플라이언스 준수 여부 등

제 33 조(정보보안 감사 수행 및 사후 관리)

① 정보보안 감사는 연 1 회 이상 전사적으로 실시하여야 하며, 인력/비용/기타 현실적인 제약으로 인하여 전사적 감사가 불가능한 경우에는 사전에 대상을 선정하여 제한적으로 실시할 수 있다.

② 보안감사는 객관성 확보를 위해 제 3 자 수행을 원칙으로 하며 전문적인 감사를 위하여 외부전문가를 보안감사 수행조직에 포함시킬 수 있다.

③ 정보보안 감사 결과 도출된 지적 사항에 대해 시정 및 조치 여부를 점검하고 향후 보안감사 계획에 반영한다

제 13 장 침해사고 대응

제 34 조(침해사고 대응 계획)

① 정보보호 책임자는 침해사고에 대한 신속하고 체계적인 대응을 위해 침해사고대응체계를 마련하여야 한다.

② 정보보호 책임자는 침해사고를 예방하기 위해 사전 모니터링 및 탐지·대응 체계를 구축하여 운영하고, 불법적인 정보유출과 보안 침해 시도에 대응하여야 한다.

③ 침해사고가 발생한 경우, 신속하게 대응하여 피해를 최소화하고 사고 경위 및 원인 등을 분석하여 필요한 조치를 하여야 한다.

제 35 조(침해사고 대응 절차)

① 침해사고 발생 시 침해사고 대응 절차에 따라 신속하게 대응한다.

② 침해사고가 조직에 미치는 영향이 심각한 경우 최고경영진까지 신속하게 보고하여야 한다.

③ 개인정보 침해사고 발생 시 법적 통지 및 신고 의무를 준수하여야 한다.

④ 침해사고 대응과 관련된 구체적인 사항은 'TYM 보안-06.침해사고대응지침'을 참조한다.

제 36 조(침해사고 모의훈련)

① 정보보호관리자는 침해사고 모의훈련 계획을 수립하고 연 1 회 이상 훈련을 실시하여야 한다.

② 정보보호관리자는 침해사고 모의훈련 결과에 대해 보고하고, 개선사항을 도출하여 침해사고 예방 및 대응체계에 반영한다.

제 14 장 재해복구 관리

제 37 조(재해복구 계획 수립)

① 정보보호관리자는 재해, 사고, 장애 발생 시 핵심 업무를 지속하기 위한 비상 대응 방안으로 위험영향도에 따른 우선순위, 처리시간에 따른 긴급도를 정의하여 재해복구 계획을 수립하여야 한다.

② 정보보호관리자는 주요 서비스 및 IT 자산의 복구목표시간과 복구목표시점을 달성할 수 있도록 비용을 고려하여 효과적인 복구전략 및 계획을 수립하여야 한다.

제 38 조(재해복구 계획의 가동)

① 재해복구 계획에 따라 위기상황 발생 시 위기대응팀을 소집하고 위기 상황의 발생원인, 발생 범위 등 관련 정보를 수집하고 분석하여야 한다.

② 위기대응팀은 업무영향분석에 따라 핵심업무 복구 우선순위, 업무복구 목표정의를 기준으로 재해복구계획을 따라 대응하여야 한다.

③ 위기상황이 종료된 후에는 대응 결과를 분석하고 재해복구 계획의 미흡점을 개선하여야 한다.

④ 정보보호관리자는 재해복구계획의 실효성을 확보하기위해 모의훈련 또는 교육을 연 1 회 이상 실시하고, 재해복구계획을 주기적으로 검토, 개선하여야 한다.

⑤ 재해복구 계획과 관련된 구체적인 사항은 'TYM 보안-07.재해복구지침'을 참조한다.

부 칙

본 정책의 시행일은 대표이사의 승인일로부터 시작된다.