정보보안관리규정

제정일자 2003.11.01
개정일자 2008.01.01
개정일자 2022.11.01
개정일자 2023.08.01

제 1 장 총 칙

제 1 조 (목적)

이 규정은 ㈜웰크론그룹(이하 '회사'라 한다) 정보자산이 사내 전산망을 이용하는 내·외부의 무단사용자에 의해 불법 유출·파괴· 변경되는 것으로부터 안전하게 보호하며, 네트워크·정보시스템 및 데이터베이스를 포함한 정보운영환경과 응용프로그램을 보다 안전하고 신뢰성 있게 운영하여 회사 전산망 사용자에게 원활한 서비스를 제공 하고자 함을 그 목적으로 한다.

제 2 조 (적용 대상 및 범위)

① 적용 대상은 사내 및 해외지사를 포함한 전부서로 한다.

② 회사의 정보자산 보호와 정보운영환경 및 응용프로그램의 운영과 제공에 관하여는 따로 규정되는 경우를 제외하고는 이 규정에 따른다.

제 3 조 (용어의 정의)

② "전산망"이라 함은 각종 정보시스템을 통신회선으로 연결하여 자료를 처리·보관하거나 전송하는 조직망을 말한다.

③ "정보시스템"이라 함은 네트워크 장비·PC·컴퓨터 서버 및 프린터 등을 말한다.

④ "시스템관리자"라 함은 시스템의 루트(root) 권한을 가지고 시스템을 운영·관리하는 자를 말한다.

④ "데이터베이스관리자"라 함은 데이터베이스를 운영·관리하는 자를 말한다.

⑤ "전산자료"라 함은 전산장비에 의해 입력·보관되어 있는 정보자료를 말하며, 백업 미디어 등 저장매체를 포함한다.

⑥ "저장매체"라 함은 자기저장장치, 광저장장치, 반도체 저장장치등 자료기록이 가능한 전자장치를 말한다

⑦ "휴대용 저장매체"라 함은 디스켓, 이동형 하드디스크(HDD), USB 메모리, Flash 메모리, CD, DVD 또는 IC 칩 등에 정보를 저장할 수 있는 모든 것으로 정보통신망과 분리할 수 있는 기억장치를 말한다

⑧ "정보보안" 또는 "정보보호"란 정보시스템 및 정보통신망을 통해 수집,가공,저장, 검색,송수신되는 정보의 유출,위변도,훼손 등을 방지하기 위하여 관리적,물리적,기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.

⑨ "전자문서"란 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송수신 또는 저장되는 정보를 말한다.

⑩ "전자정보"란 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다

⑪ “정보자산” 하드웨어(서버,워크스테이션,개인용 PC, 통신장비, 보안장비, 저장매체, 프린터 등), 소프트웨어, 응용프로그램, 개발산출물, 운영산출물 등을 말한다.

⑫ “정보보안시스템” 이란 정보의 수집,저장,검색,송신,수신 시 정보의 유출, 위조,변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.

⑬ “사이버공격” 이란 해킹, 컴퓨터바이러스, 악송코드, 랜섬웨어, 스팸메일, APT, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법춤입,교란,마비,파괴하거나 전자정보를 철취,훼손하는 공격행위를 말한다.

⑭ “정보보안담당관” 이라 함은 전산분야의 보안계획 및 운영 등의 기능을 수행하는 자로서 전산업무담당 실장(본부장)을 말한다.

⑮ “정보보안관리자” 라 함은 정보보안담당관의 임무를 위임받아 회사내 정보보안업무 실무를 총괄적으로 수행하는 부서의 팀장을 말한다.

제 2 장 위 원 회

제 4 조 (구성)

① 체계적 · 효율적인 보안정책 수립 · 심의 및 관리를 위하여 보안심사위원회(이하 '위원회'라 한다)를 둔다

② 위원회는 위원장과 정보보안담당 부위원장 1인을 두며, 그 밖의 위원은 각 팀장으로 구성한다.

③ 위원장은 정보전략실장이 겸임하며, 위원회를 대표하고 회의 업무를 총괄한다.

④ 정보보안담당 부위원장(이하 '부위원장' 이라 한다)은 전산팀장이 겸임하며, 위원장을 보좌한다.

제 5 조 (기능)

이 위원회는 제 1 조의 목적을 달성하기 위하여 다음 각 호의 사항을 심의 · 결정한다.

1. 정보보안정책 심의와 사내 정보보안의 총 관장
2. 정보보호 정책 및 총괄 계획 심의
3. 정보보안사고 처리의 책임을 심의 · 결정
4. 정보보안교육 및 정보보안준수 사항 감사
5. 기타 정보보안관련 제반업무의 총괄

제 6 조 (정보보안전담팀 구성)

① 부위원장 산하에 정보보안전담팀을 구성하여 회사에 관련된 정보보안 제반 사항을 담당한다.

② 정보보안전담팀의 구성은 전산팀을 주축으로 하며, 필요에 의하여 각 팀장들로 팀원을 구성한다.

제 3 장 보 안

제 7 조 (기본 수칙)

① 정보시스템 사용자는 개인별 사용자 계정 및 패스워드의 기밀을 유지해야 하며, 본래의 발급 목적으로만 사용하여야 한다.

② 모든 임직원은 허가 받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만 사용할 수 있다.

③ 정보시스템 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래 할 수 있는 행위를 해서는 아니 된다.
④ 제 3 항의 규정에 언급된 행위를 한 자가 발견된 경우에는 소속부서의 장 또는 정보보안전담팀에게 알려야 한다.
⑤ 정보 자산과 연관된 저작권 · 특허권 및 소프트웨어 라이센스의 사용 조건을 숙지하고 이를 준수하여야 한다.
⑥ 사내 전산망을 신설 · 변경 및 폐기하고자 하는 경우에는 회사의 사전승인을 얻어야 한다.
⑦ 외부 전산망에서 사내 전산망으로의 접근은 회사에서 승인한 정보 시스템을 제외하고는 원칙적으로 허용하지 아니 한다.
⑧ 모든 정보자산은 보안등급에 따라 분류 · 관리한다.
⑨ 회사는 주기적인 보안점검을 통해 사내 전산망 및 정보시스템의 안전성을 점검하고, 정보보안정책 및 규정의 준수 여부를 평가한다. 다만, 사내 모든 사용자는 이에 적극 협조하여야 한다.
⑩ 업무와 관련해 습득한 정보자산을 회사의 허가 없이 외부에 누출 해서는 아니된다.
⑪ 정보보안 사고의 책임은 원칙적으로 사용자 본인에게 있다.
⑫ 사이버 침해사고 발생시 대응,복구 현황을 점검 한다.

제 8 조 (보안등급 기준)

① 보안등급의 분류기준은 다음의 각 호에 따라 정한다.
1. 정보의 중요도
2. 정보(시스템)의 절취 및 불법변경 시 손실 가치
3. 정보(시스템)의 파괴 시 복구비용
4. 정보의 사용권자

② 정보자산의 보안등급 및 사용자인가는 전항의 기준에 따라 정보 자산을 보유한 부서의 장이 별도로 정한다.

제 9 조 (보안 점검)

① 정보보안전담팀은 사내 주요서버 및 각 팀의 주요 PC 서버에 대해 년 1 회 이상의 정기점검과 필요시 수시 점검을 실시한다.
② 보안점검 대상 및 분야를 해당 부서에 통보하고, 해당 부서에서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비한다.
③ 보안점검을 실시한 후 그 결과를 정보보안담당관에게 보고한 후 해당 부서에 통보한다.
⑤ 해당 부서에서는 지적 사항을 즉각 시정하고 그 결과를 위원회 정보보안담당관에게 보고한다.
⑥ 정보보안전담팀은 필요시 각 부서의 보안점검 지적 사항에 대한 시정 여부를 확인할 수 있다.
⑦ 모의 사이버테러 훈련(모의해킹, 모의침투 훈련 등)을 년 1 회 이상 정기점검과 필요시 수시 점검을 실시한다.
⑧ 스팸메일 모의훈련을 분기별 1 회 이상 자체 훈련을 진행하고, 반기별 KISA 에서 실시하는 모의훈련에 참가 한다.
⑨ 모의훈련을 통해 적발된 인원은 보안관련 온라인 교육 수강을 강제로 진행할 수 있다.

제 10 조 (보안사고의 처리)

보안사고가 발생할 경우 정보보안전담팀은 다음 각 호의 단계에 따라 적절한 조치를 취하여야 한다.

1. 침입자의 침입예방을 위하여 침입 가능성이 있는 부분을 수시로 점검하여 불법 침입자의 침입을 사전에 예방한다
2. 시스템관리자는 자신의 시스템에 비정상적인 활동이나 징후가 보이면 무단 침입자의 유무를 즉각 점검해야 한다.
3. 침입자가 현재 시스템에 침투해 해킹을 하고 있을 경우 필요한 조치를 즉각 취하고 보고하여야 한다.
4. 침입자를 몰아냈거나 로그파일의 분석을 통해 침입한 흔적이 발견된 경우 즉시 보고하고, 보안진단도구나 체크리스트를 이용하여 정보자료의 이상유무를 점검하여야 한다.
5. 정보보안관리자는 정보보안 사고 발생 시 즉시 피해확산 방지조치를 취하여야 한다. 이 경우, 사고원인규명 시까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포메하여서는 아니 된다.
   ① 일시 및 장소
   ② 사고원인 및 피해 현황 등 개요
   ③ 사고자 및 관계자의 인적사항
   ④ 조치내용 등
6. 정보보안관리자는 사고원인 및 피해 현황을 파악하고, 재발장비 대책의 수립,시행 등 사고조사 결과에 따라 보호대책을 마련하고 조치하여야 한다.

제 11 조 (보안 교육)

① 사내 의사결정자 · 사용자 및 시스템 관리자를 대상으로 정보보안 교육을 실시한다.

② 보안에 대한 인식을 제고하고 사용자와 시스템 관리자의 부주의나 고의에 의한 보안사고를 최소화한다.

③ 보안교육은 년 1회의 정기교육과 필요에 따라 수시교육을 실시한다.

제 4 장 정보시스템 관리

제 12 조 (사용자 정의) 정보시스템을 사용할 수 있는 자는 다음 각 호와 같다.

1. 회사의 모든 임직원
2. 인사위원회가 특별히 사용을 인정한 자

제 13 조 (적절성 확보)

사내 정보시스템 이용자는 정보시스템 사용에 있어 적절성을 유지하여야 한다. 다만, 다음 각 호에 해당하는 경우에는 부적절한 사용으로 간주하여 제재조치를 취할 수 있다.

1. 타 사용자의 계정 및 패스워드를 허가 없이 사용한 경우
2. 타 사용자의 정당한 사용을 방해한 경우
3. 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 행위
4. 일반사용자가 "root" 패스워드 또는 타 사용자의 패스워드를 획득 하고자 해킹하는 행위
5. 내부의 중요 전산정보를 불법으로 외부에 유출한 경우

6. 외부의 불법사용자에게 계정 및 패스워드를 제공한 경우
7. 사용자 계정 및 패스워드를 상호 공유하는 행위
8. 시스템관리자가 특별한 사유 없이 "root"패스워드를 일반사용자와 공유한 경우
9. 허가된 보안등급 이상의 자료를 무단유출 하거나 읽고 쓰는 행위
10. 인터넷을 통해 자살 사이트나 음란 사이트 등 반사회적인 유해사이트에 접속·개설·열람하는 경우
11. 보안점검의 지적 사항에 대해 즉각적인 시정을 취하지 않는 경우

제 14 조 (사용자 제재)

① 제 13 항에 규정된 사항에 해당할 경우에는 사용자의 계정을 회수·삭제하여 정보시스템의 사용을 제한 또는 금지하며, 그에 따른 구체적 제재 사항은 위원회에서 심의·결정한다.

② 정보시스템의 불법사용으로 회사에 해를 끼치거나 명예를 훼손시 시켰을 경우에는 다음 각 호의 제재 조치를 취할 수 있다.

1. "정보통신망 이용촉진 등에 관한 법률"(법률 제 5,835 호)에 의한 법적 조치
2. 취업규칙 제 17 조에 따른 징계 조치
3. 정보시스템의 손해발생에 대한 손해배상 청구

제 15 조 (정보시스템 보안)

① 직원은 PC 등 정보시스템을 사용하거나 본인계정으로 정보통신망에 접속하는 것과 관련한 보안 책임을 가진다

② 정보보안관리자는 서버,네트워크 장비 등 부서 공통으로 사용하는 정보시스템의 운영과 관련한 보안 책임을 가진다.

③ 정보보안관리자는 해당 부서 정보시스템의 변경 현황을 유지하여야 하며 정보보안관리자 요청 시 사본을 제출하여야 한다.

④ 정보보안관리자는 정보시스템이 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 하며, 보안취약점을 제공할 수 있는 다음 각 호의 프로그램 설치를 제한하여야 한다.

1. P2P, 웹하드 등 파일 공유 프로그램
2. 사외 메신저(SNS 포함), 웹메일 등 자료를 외부로 전송할 수 있는 프로그램
3. 업무와 관련 업는 웹 사이트(증권, 게임 등)
4. 비인가 프로그램
5. 출처가 불분명한 응용프로그램
6. 업무상 불필요한 프로그램

⑤ 정보보안관리자는 소관 시스템의 안정적 운영을 위해 다음 각 호에 따라 관리해야 한다.

1. 신규로 설치되는 시스템의 취약점 점검 및 조치
2. 시스템의 운영체제 등 최신 패치 실행
3. 설치,운영 중인 시스템의 수시 보안취약점 점검 및 조치

⑥ 정보보안담당관은 제 1 항부터 5 항까지에 명시된 정보시스템 운용과 관련한 보안취약점을 발견하거나 보안대책 강구가 필요하다고 판단할 경우, 정보보안관리자에게 개선을 요구할 수 있다.

제 16 조 (PC 등 단말기 보안관리)

① 단말기 사용자는 PC,노트북,스마트기기 등 단말기(이하 “PC 등” 이라 한다) 사용과 관련한 일체의 보안관리 책임을 가진다.

② PC 등에 적용되는 사용자계정(ID) 및 비밀번호의 취급관리는 17 조(사용자계정 관리)와 제 18 조 (비밀번호 관리)의 사항을 준용한다.

③ 사용자는 PC 등의 보안관리를 위해 다음 각 호의 사항을 준수하여야 한다.

1. 컴퓨터명은 SS+한글이름으로 설정한다.
2. PC 기동 시 도메인 서버에서 제공하는 도메인 암호를 이용하여 로그인한다.
3. 화면 보호기는 PC 미사용 5 분이 경과하면 작동시켜야 하며 패스워드를 설정한다. 또한 화면보호기 대기시간을 1 분으로 설정, 도메인 정책으로 전체 적용한다.
4. 장시간 자리를 비울 때는 전원을 끈다.
5. 자신의 업무에 사용하는 응용프로그램은 시스템 보안관리자의 허락 없이 무단으로 타인에게 복사해 주어서는 아니 된다.
6. IP 주소 임의 변경 금지 한다.
7. 최신 보안업데이트, 바이러스 치료 프로그램(백신프로그램) 등 보안 프로그램 설치 및 주기적인 검사를 진행한다.

④ 정보보안관리자는 비인가자 PC 등을 무단으로 조작하여 전자정보를 유출하거나, 위조,변조 및 훼손시키지 못하도록 다음 각 호에 따른 보호대책을 강구하여야 한다.

1. 제 17 조(사용자계정 관리)에 따라 장비별, 사용자별 비밀번호 설정 관리
2. 백신프로그램 등의 운용
3. P2P 등 업무와 무관하거나 보안에 취약한 프로그램의 사용금지

⑤ 정보기술팀에서는 PC 등 교체,반납,폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 완전삭제 등 보안조치를 수행하고, 정보보안관리자 요청 시 결과를 제출하여야 한다.

⑥ PC 등의 외부 반출을 제한하며, 외부 업무용으로 사용하는 PC 등에 한하여 정보기술팀 직원의 책임하에 반출 할 수 있다.

⑦ 정보기술팀에서는 PC 등의 반출,반입 통제조치를 수행하여야 한다.

⑧ 정보보안관리자의 요청 시 정보기술팀에서는 반출,반입 현황을 제공하여야 한다.

⑨ 회사의 모든 임직원은 회사에서 지급한 PC 등 인가된 전산 장비만을 사용하여야 하며 개인용 노트북 또는 공유기 등의 사용을 금한다.

⑩ 퇴근 및 외근 시에는 작업 중인 데이터 손실을 방지하기 위해 저장을 완료하고, 반드시 개인 PC 의 전원을 끄고 퇴근 및 외근을 가야 한다.

제 17 조 (사용자계정 관리)

① 정보보안담당관은 사용자계정(ID)의 비인가자 도용 및 정보시스템 불법접속 등을 방지하기 위해 다음 각 호의 사항을 조치하야여 한다.

1. 신규 사용자계정 생성시 신청서 작성, 신원확인, 기안품의 등의 절차를 거처 발급
2. 직무변경, 퇴직 등 인사이동이 있을 경우 관련 정보시스템 접근권한을 조정
3. 사용자별, 그룹별 접근권한 부여 및 사용자계정 공용 금지
4. 외부 사용자의 계정부여는 불허하되, 부득이한 경우 유효기간을 설정하는 등의 보안조치 이후 허용
5. 비밀번호 등 사용자 식별, 인증 수단이 없는 사용자계정 사용금지
6. 장기간 사용하지 않는 휴면계정을 점검하여 불필요시 삭제

7. 사용자계정을 주기적(년 1 회)으로 점검하여 접근권한 재검토

② 정보시스템의 계정은 사용목적 및 권한에 따라 관리자계정과 사용자 계정으로 구분하여 관리하여야 한다.

③ 관리자계정은 관리자로 지정된 자만이 사용할 수 있으며, 타인에게 대여할 수 없다. 다만, 업무상 필요에 의해 타인에게 대여한 경우에는 회수 후 즉시 비밀번호를 변경하여야 한다.

④ 정보기술팀에서는 소관 정보시스템별 계정발급현황을 관리하여야 한다.

제 18 조 (비밀번호 관리)

① 비밀번호는 다음 각 호의 사항을 반영하여 숫자와 영문자, 특수문자 등을 혼합하여 9 자리 이상으로 정하여야 한다. 다만, 개인 PC 로그인 비밀번호는 영문자와 숫자를 혼합하여 6 자리이상으로 정한다. 또한 정보시스템에서 기능을 지원하지 않는 경우에는 예외로 한다.

1. 사용자계정(ID)과 동일하지 않을 것
2. 개인신상 및 부서명칭 등과 관계가 없을 것
3. 일반 사전에 등록된 단어 또는 추측하기 쉬운 단어는 사용을 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 말 것
5. 사용된 비밀번호는 재사용하지 말 것
6. 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지
8. 비밀번호에 유효기간을 90 일로 선정하여 주기적으로 변경할 것

② 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

③ 비밀이나 중요자료는 자료별 비밀번호를 부여하여야 한다.

제 5 장 네트워크 관리

제 19 조 (전산망 관리)

① 네트워크관리는 일관성과 기밀성을 위해 통합관리를 원칙으로 한다.

② 운영부서의 관리자는 네트워크 신규설치 및 변경 시 정보보안전담 팀에 변경정보를 통보해야 한다.

③ 네트워크 IP ADDRESS 는 사용자가 임의로 변경할 수 없다.

④ 정보보안관리자는 라우터, 스위치 등 네트워크 장비 운영과 관련하여 다음 각 호의 보안조치를 강구하여야 한다.

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되 불가피할 경우 장비 관리용 목적으로 접근제어솔루션(NAC)의 통제에 따라 내부 지정된 단말기 IP 주소에서만 접속 허용
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
3. 최소 설치 시 보안취약점을 점검하여 제거하고 주기적으로 보안 패치 실시
4. 불필요한 서비스 포트 제거

⑤ 라우터 패스워드는 제 17 조에 규정된 계정관리에 따른다.

⑤ 인터넷을 이용한 모든 외부로부터의 접근은 원칙적으로 방화벽을 통해서만 접근 가능하도록 한다.

⑦ 외부접속자의 "root" 로그인은 허용하지 않는다.

⑧ 일정횟수 접속실패 시 접속을 차단하고 관련 정보를 로그에 기록한다.

제 20 조 (방화벽 관리)

① 방화벽 시스템에는 슈퍼유저 이외의 어떤 계정도 두지 않음을 원칙으로 하되, 예외적인 사항에 한하여는 정보보호담당관이 결정한다.

② 방화벽 시스템에는 O/S, 방화벽 소프트웨어 이외에는 어떤 소프트웨어도 설치하지 않는다.

③ 외부에서 내부로의 모든 접속시도는 LOG 관리되어야 하며, 세 번 이상의 패스워드 입력 오류 시에는 해당 사용자로부터의 접속 시도를 차단한다.

제 6 장 서버 관리

제 21 조 (운영 및 관리)

① 신규 채용된 직원의 계정 등록요구 시 시스템 관리자에게 사용목적 등을 제출하도록 한다.

② 휴직자의 계정은 휴직기간 동안 잠정 폐쇄를 원칙으로 한다.

③ 퇴직자는 사직원 제출 시 사용자 계정을 반납하도록 한다.

④ 시스템 관리자는 최소 월 단위로 사용자의 패스워드를 체크해 취약한 패스워드가 발견될 경우 당사자에게 통보하여 변경을 요구할 수 있다.

⑤ 취약한 패스워드를 사용한 계정에 대해서는 경고를 하되, 2 회 이상의 경고를 받고도 변경하지 않을 경우에는 1 개월 동안 계정을 폐쇄할 수 있다.

⑥ 시스템 개발 및 운영부서의 장은 응용프로그램 개발계획 단계에서 보안정책에 근거한 응용프로그램 개발을 지시하고, 이를 위반할 경우에는 개발을 중지시킬 수 있다.

⑦ 슈퍼유저의 권한은 정보보안업무 담당자/시스템 관리자로 제한한다.

⑧ 장애복구나 점검을 위해 루트 권한을 위임할 경우에는 시스템 관리자 입회하에 작업을 실시하고, 작업종료 후 루트계정과 패스워드를 변경한다.

⑨ 백업지침은 별도로 정하며, 반드시 지침에 따라 주기적인 백업을 실시한다.

⑩ 각 부서는 백업 미디어별로 적절한 사용연수를 정하여 노후된 백업미디어에 대해서는 사용하지 아니 한다.

제 22 조 (보안관리)

① 전체 시스템에 대한 보안관리와 전반적인 방향설정 및 주기적인 보안점검은 정보보안전담팀에서 실시한다.

② 개별 서버에 대한 보안관리는 각 서버의 관리자가 담당한다.

제 23 조 (계정관리)

① 사용자 계정 분류는 그 사용목적에 따라 분류하고 그 기준은 따로 정한다.

② 사용자별 또는 그룹별로 접근권한을 부여한다.

1. ERP 시스템으로의 접근권한은 동일 업무내의 권한은 팀장의 승인을 득하고,
2. 타 팀의 업무인 경우 본부장의 승인을 득한 후 부여한다.

③ 패스워드가 없는 계정은 사용을 금지한다.

④ 일정회수 접속 실패시 사용을 금지한다.

⑤ 사용자 계정절차의 등록·변경 및 폐기는 다음을 따른다.

1. 사용자 계정은 사용자 등록이나 변경 또는 폐기 신청서를 작성 한 후에 시스템 관리자에게 통보하되, 사용목적 등의 사유를 명확히 해야 한다.

2. 시스템관리자는 내용을 검토한 후에 사용자 계정을 등록이나 변경 또는 폐기하고 사용자에게 그 사실을 통보한다.
3. 사용자 계정을 등록하거나 변경 또는 폐기할 경우에 일반적인 사항은 월 단위로 부서장에게 사후 보고한다. 다만, 특별한 상황이 발생할 경우에 한하여 부서장의 허가를 받은 후에 작업을 실시한다.

제 5 장 전산자료 및 데이터베이스 관리

제 24 조 (자료의 관리)

① 데이터베이스 로그인 계정 관리기준은 DBMS 관리자(DBA)·응용프로그램 개발자 및 사용자에 따라 권한을 차등 부여하고, 패스워드는 암호화된 형태로 존재하도록 한다.
② 데이터베이스의 무결성 유지를 위해 데이터베이스의 수정은 적법한 인가자에 의해서만 이루어져야 하며, 물리적인 재해로부터의 보호를 위해 주기적으로 백업하여야 한다.
③ 데이터베이스에 대한 모든 접근은 감사기록을 유지하되, 일반사용자의 감사기록에 대한 접근은 제한해야 한다.
④ 데이터베이스 관리자(DBA)는 누가 어떤 필드, 레코드 수준에서 접근할 수 있는가를 정의해야 한다.
⑤ DBMS 는 시스템과는 별도의 사용자 인증기능을 수행해야 한다.
⑥ 데이터베이스의 데이터는 응용프로그램을 통해서만 접근한다.
⑦ 별도지침에 의해 중요자료로 분류된 자료 및 데이터베이스는 데이터의 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제 25 조 (자료의 백업 및 보관)

① ERP 서버, 데이터베이스 서버, ERP 소스 서버의 백업은 1일 백업을 원칙으로 시행한다.
② 1항에서 일일 백업된 DATA 를 다른 곳에 2차 백업을 진행한다.
③ PC 의 데이터는 현업의 팀장이나 본부장이 요청하는 경우, 또는 퇴사자 발생시 현업에서 요청시 별도 백업을 진행한다.
④ 별도지침에 의해 중요자료로 분류된 자료의 이용 및 변경은 부서장의 허가와 관리책임자의 입회 하에 이용 및 변경할 수 있다.

제 26 조 (자료의 파기)

① 별도지침에 의해 중요자료로 분류된 자료의 파기는 자료보관책임자의 입회하에 담당자가 파기를 실시하고, 자료관리대장의 파기 확인란에 입회자는 파기 확인을 한다.
② 자기테이프 등의 자기매체 자료의 파기는 컴퓨터를 이용하여 내용을 완전히 삭제하고, 자료접근이 불가능해 내용을 지울 수 없는 자기매체의 자료는 소각 또는 용해 등의 방법으로 파기한다.
③ 소규모의 전산파지는 분쇄기를 이용하고, 대규모의 파지는 소각시킨다.

제 6 장 응용프로그램 관리

제 27 조 (응용프로그램 개발)

① 모든 응용프로그램은 접근하는 데이터의 정보등급에 따라 해당 응용프로그램의 보안등급을 설정한다.

② 응용프로그램의 계획서 및 설계서는 보안관리규정에 근거하여 보안대책이 마련되어야 하며, 프로그램 개발 시에 이를 반영해야 한다.
③ 별도지침에 의해 중요자료로 분류된 응용프로그램은 정보보안을 위해 사용자계정 및 패스워드를 설정해야 한다.
④ 응용프로그램에서 사용하는 사용자계정·패스워드 및 기타 전산망 접근과 관계된 중요정보는 소스코드로부터 분리하여 1차 인식이 불가한 암호화된 형태로 존재해야 한다.
⑤ 별도지침에 의해 중요자료로 분류된 응용프로그램은 개발시 시스템 사용에 대한 로그 정보를 관리함을 원칙으로 한다.

제 28 조 (응용프로그램 운영)

① 응용프로그램 운영자는 응용프로그램 사용자 계정에 대한 패스워드 변경을 최소 3개월에 1회 이상 실시해야 한다.
② 응용프로그램 운영자는 시스템 사용에 대한 로그 정보를 주기적으로 분석하여 자료의 불법접근 및 변조에 대한 위험성을 사전에 방지해야 한다.
③ 응용프로그램의 버전관리는 소스프로그램과 실행프로그램의 버전이 일관성을 유지하도록 한다.
④ 개발된 응용프로그램의 복제는 시스템관리자의 사전양해와 입회하에 실시해야 한다.
⑤ 응용프로그램의 추가·삭제 또는 변경은 부서장의 허가를 받은 후에 시스템 관리자에 의해 실시되어야 한다.
⑥ 운영중인 시스템에는 응용프로그램의 소스프로그램을 설치하지 않는 것을 원칙으로 한다.
⑦ 별도지침에 의해 중요자료로 분류된 응용프로그램은 가동 전 정보보호전담팀의 보안검증을 받아야 한다.

제 6 장 시스템실 운영·관리

제 29 조 (시스템실 시설기준)

① 물리적 출입통제를 통해 인가된 직원만 출입 할 수 있도록 한다.
② 자동화재경보 설비를 설치하고, 할로겐 가스 등 소화 시 장비에 피해를 주지 않는 자동 소화 설비를 설치한다.
③ 정전에 대비하여 별도의 전원공급 시설을 둔다.
④ 온·습도를 적절히 유지할 수 있는 시설을 갖춘다.

제 30 조 (시스템실 운영 및 관리)

① 시스템실의 운영을 담당하고 있는 부서장은 시스템실 사용 및 운영에 관한 절차 및 방법을 규정하고, 담당자들이 이를 숙지하도록 한다.
② 시스템실의 운영자는 운영일지 및 장애일지를 작성해야 한다.
③ 시스템 운영자는 주기적으로 로그화일을 분석해야 하며, 시스템에 이상이 발견되었을 경우에는 보안사고처리 지침에 따라 즉시 조치를 취하고 이를 정보보안전담팀 및 부서장에게 보고해야 한다.
④ 시스템실에는 출입자 명부를 비치하고 비인가자의 출입을 통제해야 한다.

⑤ 시스템실 · 자료보관실 및 통신실은 관리책임자를 지정하고 자료 또는 장비별로 취급자를 지정 운영해야 한다.

제 7 장 기 타

제 31 조 (규정개정) 이 규정의 개정은 위원회의 의결을 거쳐 대표이사의 승인을 얻어야 한다.
제 32 조 (시행세칙) 이 규정의 운용에 필요한 세부사항은 시행세칙으로 따로 정할 수 있다.
제 33 조 (준용) 기타 이 규정에 명시되지 아니한 사항은 회사의 관계 규정에 준한다.

부 칙

1. 시 행 일
(1) 본 규정은 2003 년 11 월 1 일부터 제정, 시행한다.
(2) 이 규정은 사명 변경으로 2008 년 1 월 1 일부터 변경 시행한다.
(3) 본 규정의 추가 및 변경으로 2022 년 11 월 1 일부터 변경 시행한다.
(4) 본 규정의 추가 및 변경으로 2023 년 08 월 1 일부터 변경 시행한다. - 끝 -