개정 이력

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

차수	제(개)정 일자	시행일자	주요 개정 내용
1	2017-09-13	2017-09-13	초도 제정
2	2023-12-01	2023-12-01	디오토 상호변경
3	2023-12-05	2023-12-05	소프트웨어 설치 절차 추가
4	2024-08-01	2024-08-01	넥스오토 상호변경
5	2024-08-01	2024-08-01	비밀번호 운영 절차 추가
6	2025-02-03	2025-02-03	비인가 소프트운영 절차 및 보안패치 운영절차 추가

목 차

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

1. 개요

1.1 목적

본 지침서는 사내 전 임직원 및 외부 협력업체 인원이 보안지침 및 절차에 따라 업무를 수행하게 함으로써, 회사의 정보자산을 안전하게 활용하도록 하며 정보자산에 대한 위협행위(정보유출, 인터넷 침해사고 등)로부터 피해를 방지함을 목적으로 한다.

1.2 적용범위

당사 소유의 정보자산을 이용하는 임직원과 계약직, 임시직을 포함한 외주인력을 대상으로 한다.

1.3 책임 및 권한

1.3.1 전사보안책임자

① 회사의 정보자산에 대한 전반적인 관리책임을 가진다.

② 본 지침서에 규정된 사항이 적절히 이행되는지 관리할 책임이 있다.

1.3.2 기술보안담당자

① 사용자보안지침을 작성하며 주기적으로 개정, 검토하여 이를 전 회사 사용자들에게 공지하여야 한다.

② 사용자 PC에 대한 보안성을 평가하고 보안규정 미준수 사용자에게 개선하도록 요구할 책임과 권한을 가진다.

1.3.3 정보자산관리 담당자

① 기술보안담당자와 겸임할 수 있다.

② PC 등 개인용전산장비의 도입, 폐기 및 소프트웨어의 설치와 폐기에 대한 관리책임이 있다.

1.3.4 PC 사용자

① 본인의 PC를 보호할 의무와 책임을 가진다. 본 지침에 수록된 내용을 지키지 않음으로써 발생하는 모든 회사의 손실에 대해서는 사용자가 책임을 진다.

② PC의 비인가적 사용을 금하며, 임의의 포맷을 금한다.

③ PC의 정보보호 기능 설정 및 활용을 하여야 한다.

④ PC 내 기밀정보를 보호해야 한다.

⑤ 바이러스/악성코드 감염 예방을 하여야 한다.

⑥ 사용 소프트웨어에 대한 지적재산권을 준수하여야 한다.

2. 사용자 윤리

- 회사의 업무시스템은 개인적인 사업목적이나 이익을 위하여 사용할 수 없으며, 회

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

사 업무용으로만 사용하여야 한다.
- 회사의 업무시스템 관련자료를 무단으로 변조하거나 훼손하지 않아야 한다.
- 회사의 모든 정보자산은 관리자의 승인(확인)없이 외부로 무단반출 및 오픈하지 않는다.
- 저작권을 침해할 수 있는 자료를 회사 통신망을 통하여 무단으로 배포하지 않는다.
- 임직원은 스팸메일, 행운의 편지, 불건전한 저속한 메일(자료) 등 미풍양속을 해치거나, 물의를 야기할 수 있는 정보 또는 메일을 회사 통신망을 통하여 유통시키지 않는다.
- 회사 내에서 불건전한 인터넷 사이트를 열람 또는 파일을 다운로드 하지 않는다.
- 회사 통신망을 이용하여 다른 회사 및 기관, 개인에 피해를 가할 수 있는 불법적인 행위를 하지 않는다.
- 타 회사나 기관의 비밀정보를 회사 내 시스템에 보관할 수 없다.

3. 사용자 보안업무 절차

3.1 PC 보안

3.1.1 개인 소유의 PC, Tablet PC, CD-Writer, 외장형저장장치, 데이터케이블 등 전산장비) 회사에 반입 및 사용할 수 없으며, 업무상 특정 목적이 있는 경우 승인절차에 의거 사용할 수 있다.

3.1.2 회사소유 자산은 개인목적으로 반출할 수 없으며, 출장, 이동영업 및 수리를 위한 반출은 승인절차 후 반출하여야 한다.

3.1.3 외부에 내부정보 제공 시는 반드시 승인절차를 거쳐야 하며, 미 승인된 정보에 대한 책임은 전적으로 사용자에게 있다.

3.1.4 손상된 PC의 복구를 위해 외부에 반출할 경우 저장장치에 업무와 관련된 주요 파일이 있는 지 확인하여 백업 후 제거해야 한다. 다만, 디스크의 장애로 데이터복구를 위해 반출할 경우에는 중요데이터 정보 소유자 입회 하에 디스크 복구 작업을 진행하여 정보유출 가능성을 차단한다.

3.1.5 PC 로그인 및 화면보호기 패스워드를 설정하여야 하고, 화면보호기 암호시간은 10분으로 설정한다.

3.1.6 패스워드는 영문자 및 숫자, 특수문자 포함 8자리 이상이어야 하며, 3개월 주기로 변경하여야 한다.

3.1.7 패스워드는 자신과 관련된 정보를 이용하여 패스워드를 만들지 않는다.

3.1.8 패스워드는 타인이 추측하기 어려운 것을 사용하여야 하고, 본인만이 알고 있어

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

야하며 타인과 공유해서는 안된다.

3.1.9 패스워드는 노출되지 않아야 하며, 노출 시 즉시 변경하여야 한다.

3.1.10 한번 사용된 패스워드는 6개월 간 재사용이 금지된다.

3.1.11 공유 폴더 사용 시에는 업무적으로 인가된 사용자만 접근 가능하도록 공유 설정 후 사용하여야 하며, 사용 목적이 완료된 경우에는 공유 설정을 즉시 해제 하여야 한다. 공유 폴더 설정 시 기본값으로 되어 있는 Everyone, Domain Users 계정정보는 삭제하여 비인가자의 접근을 방지한다.

3.1.12 주기적으로 보안패치업데이트를 실시하여야 한다.

3.1.13 병가나 장기 휴가와 같이 1개월 이상 사용하지 않을 경우 사용자계정 신청서를 작성하여 계정 사용중지를 서버 운영자에게 요청하여야 한다.

3.1.14 공용PC는 관리자를 지정하여 주기적으로 관리하여야 하며, 업무 자료는 사용 후 즉시 삭제하여야 한다.

3.1.15 공용PC는 보안 시스템을 반드시 설치하여야 한다.

3.1.16 공용 PC에는 보안문서를 저장할 수 없다.

3.1.17 노트북을 이용하여 외부에서 내부 네트워크에 연결할 수 없으며, 특정 업무목적으로 접근이 필요할 시는 네트워크보안지침을 따른다.

3.1.18 노트북에 저장되어 있는 업무자료는 비밀번호 설정 또는 암호화(DRM 등) 조치를 통하여 분실/도난 사고 발생 시 비인가자의 불법 열람 및 외부 공개으로부터 보호되어야 한다.

3.1.19 노트북은 절도로부터 보호될 수 있도록 취급상 주의를 기울이며 안전케이블 또는 잠금 장치를 사용하여야 한다.

3.1.20 노트북을 출장 등의 사유로 회사 외부로 반출할 경우 해당 자산의 관리자로부터 승인을 얻어야 한다.

3.1.21 장비의 폐기 시는 회사에서 지정한 전용S/W 등을 통해 정보를 완전히 삭제해야 한다.

3.2 소프트웨어 보안

3.2.1 PC에는 회사 업무용 목적으로 사용되는 프로그램만 설치한다.

3.2.2 지적재산권을 준수하여, 정품S/W만 설치되어야 하며, 불법 S/W사용에 대한 책임은 본인에게 있다.

3.2.3 PC에 설치 시 바이러스나 악성코드처럼 동작할 가능성이 있는 비인가 S/W는 임의 설치 및 사용해서는 안되며, 업무적으로 사용이 필요할 경우 회사에 요청

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

하여 동일한 기능이 있는 공식 S/W를 구매하여야 한다.

3.2.4 사용중인 S/W에 보안상 문제가 발견 혹은 공지되었을 경우에는 즉시 문제 해결된 최신 프로그램이나, 패치를 적용하여야 한다.

3.2.5 회사에서 제공한 악성코드차단 솔루션을 설치하여야 하며, 최신 업데이트를 하여야 한다.

3.3 모바일 기기 보안

3.3.1 모바일 기기를 사용하여 업무를 수행하는 경우 회사에서 보호조치를 제공하여야 한다.

3.3.2 모바일 기기에 회사 내 정보가 저장되지 않도록 통제하고, 기기간 연결매체를 통제할 수 있는 기술을 적용하여 승인되지 않은 모든 접속을 차단한다.

3.3.3 메일을 사용하여 회사정보를 수신하는 경우 첨부파일 저장을 제한한다.
(모바일 기기에 메일을 사용하여 회사정보를 수신하는 경우 첨부파일을 저장해서는 안된다.)

3.4 전자메일 보안

3.4.1 업무에 필요한 사항은 회사에서 제공하는 전자메일 서비스를 반드시 사용하여야 한다.

3.4.2 전자메일 이용 시에는 바이러스나 절취와 같은 위험에 대해서 항상 인식을 하여야 하고, 발신인이 불분명한 의심스러운 메일은 열지 말고 삭제하여야 한다.

3.4.3 전자메일에 민감하거나 중요정보를 첨부할 경우에는 문서에 패스워드를 부여하거나 암호화하여 전송하여야 한다.

3.4.4 PC방과 같이 많은 사람들이 이용하는 공공 장소에서는 업무에 관계되는 메일을 확인하거나, 수신 또는 전송하는 것은 긴급한 업무 처리 등의 불가피한 경우를 제외하고는 자제하여야 한다.

3.5 정보자산관리

3.5.1 PC 내에 저장된 모든 문서(진행 중인 문서 포함)는 정보자산분류 기준을 적용하여야 한다.

3.5.2 비밀 또는 극비 문서의 경우 반드시 보안이 적용된 별개의 저장매체를 통하여 백업을 실시하고, 별도의 장소에 보관하여야 한다.

3.5.3 보안 문서의 경우 이동 저장매체에 저장시 보안조치(암호화, 보안USB 등)가 수

반되어야 한다.

3.5.4 비밀 또는 극비 문서는 별도의 시건된 장소에 보관하여야 한다.

3.5.5 극비 문서가 저장된 폴더는 공유할 수 없다.

3.5.6 PC내에 중요 자료를 저장할 경우에는 중복되게 보관하지 않는다. (무결성 유지)

3.5.7 보안 문서는 외부로 공중 네트워크(인터넷)을 거쳐 전송하는 것은 불허하며, 부득이 전송이 필요한 경우는 관리자의 승인을 받아야 한다.

3.5.8 허가 받지 않은 정보자산의 유출여부를 검사하는 경우 검사에 응해야 한다.

3.5.9 외부에 내부정보 제공 시는 승인절차를 거쳐야 하며, 미 승인된 정보에 대한 책임은 전적으로 사용자에게 있다.

3.5.10 S/W 설치 및 사용

① 사용자는 본인이 관리하는 PC에 대해서 업무에 필요한 S/W를 신청할 수 있으며, 아래의 절차를 따라야 한다.

② 절 차

→ S/W 설치 신청서 작성(사용자) → 사용 용도 및 필요성 검증 (전산팀) → 자체 보유 S/W 즉시배포(이력관리) → 신규 프로그램 전산팀 필요수량 검토 후 업체 선정 정식 라이선스 구매 후 배포 (이력관리)

3.6 인터넷 보안

3.6.1 인터넷으로 통하는 모든 접근은 회사 보안 정책을 준수하는 것으로 인증되고 승인된 회사의 보안시스템을 통해야 한다.

3.6.2 웹브라우저는 취약점이 보완된 최신 버전을 사용하여야 한다.

3.6.3 회사의 승인을 득하지 않고 통신선을 개설하거나, 인터넷 통신이 가능한 프로그램을 가동하여 회사에서 지급한 PC 또는 서버를 임의로 인터넷에 오픈 할 수 없다.

3.6.4 사용자 정보가 암호화되지 않는 사이트에 접속하여 문제가 발생할 경우 사용자 본인에게 책임이 있다.

3.6.5 회사 통신망의 성능저하를 초래할 수 있는 업무상 관련이 없는 인터넷 사용을 금한다. 인터넷 상의 특정 사이트에 대해서 회사는 정상적인 경영활동을 위해 회사에서의 접속을 금지할 수 있다.

3.6.6 외부 커뮤니티 싸이트(SNS 등)에 회사업무에 관한 내용을 등록하지 않는다.

3.6.7 불법적인 도박 사이트, 성인 사이트 등의 접속은 회사가 정책을 정의하고, 그 정

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

책에 따라 접속을 차단 하도록 한다. (예: 업무 시간에는 도박 및 성인 사이트 접속 금지 정책 등)

3.6.8 회사는 인터넷의 FTP 사이트 및 웹하드 사이트를 통한 정보유출을 방지하기 위하여 접속을 차단할 수도 있으며, 업무적으로 필요한 사용자에 대해서는 승인된 절차를 거쳐 사용하도록 한다.

3.7 Clean Desk

3.7.1 사용자는 본인이 관리하는 회사 중요 서류 및 저장매체는 비인가 접근의 방지를 위하여 퇴근 시 시건 장치가 된 장소에 보관하여야 한다.

3.7.2 퇴근 또는 자리 이석시 중요 자료 및 저장매체를 방치하지 않고 정리 정돈 상태를 유지하여야 한다.

3.8 비밀번호 운영절차

3.8.1 비밀번호 생성

① 비밀번호 최초 생성 시 최소 길이는 8자리 이상으로 하고, 영문, 숫자, 특수문자 중 최소 2가지 조합으로 생성한다.

② 비밀번호는 두 자리 이상 연속된 값을 사용 불가하며, 불규칙적인 암호로 생성하도록 한다.

3.8.2 비밀번호 변경

① 비밀번호 변경주기는 90일 이내로 하며, 변경하지 않을 경우는 접속을 제한하도록 한다.

② 변경할 비밀번호는 직전 2회 변경된 비밀번호는 사용할 수 없다.

3.8.3 비밀번호 분실

① 비밀번호 분실 시 즉시 기술담당자에게 보고하고 해당 계정 사용중지 요청을 한다.

② 비밀번호를 새로 발급하고자하는 경우는 비밀번호 발급사유서를 작성하여 기술보안담당자에게 직접 제출하고 본인확인을 거쳐 발급받도록 한다.

③ 새로 발급할 임시 비밀번호는 연속되지 않는 임의의 숫자, 대/소문자가 포함된 임의의 문자 및 특수문자가 모두 포함되어 8자리로 생성되도록 한다.

3.8.4 관리자 패스워드 유지관리

① 관리자 패스워드는 비밀등급으로 관리하며, 해당 업무 시스템의 관리자로 선임되어있는 자 외에 타인에게 절대 노출되지 않도록 한다.

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

② 관리자 접속정보 등은 비밀등급으로 표기하고 시건장치하여 보관하도록 한다.

3.8.5 모든 사용자 및 이용자 패스워드 유지관리 및 교육

① 모든 사용자 및 이용자는 패스워드를 타인이 식별 가능하도록 보관 및 방치해서는 안된다.

② 보안담당자는 패스워드 관리절차에 관한 교육을 보안교육 시 실시하도록 한다.

3.9 비인가 소프트웨어 통제 운영절차

3.9.1 통제대상

① 사내에 사용되고 있는 개인 업무용 PC 및 서버 등 소프트웨어가 설치될 수 있는 모든 기기 및 사용자를 대상으로 한다.

3.9.2 통제항목

① 개인업무용 PC

a. 운영체제 라이선스
b. 문서작업 프로그램 라이선스
c. 백신 프로그램 라이선스
d. 기타 프로그램의 라이선스

② 서버

a. 운영체제 라이선스
b. 데이터베이스(DB) 라이선스
c. ERP, 인증서버의 라이선스
d. 백신 프로그램 라이선스
e. 기타 프로그램의 라이선스

③ 특수프로그램

a. 도면작업(CAD, CATIA 등) 프로그램 라이선스

3.9.3 모니터링

① IT 자산관리 툴 또는 그에 준하는 시스템을 활용하여 실시간 프로그램 설치내역을 확인한다.

② 상기 시스템에 갖춰져 있지 안흔 경우 월 1회 불시 샘플링을 점검 한다.

③ 연 1회 사내 모든 PC 및 서버의 소프트웨어 전수 검사를 실시하여 비인가 소프트웨어 정리를 실시한다.

3.9.4 위반 시 절차

① 비인가 소프트웨어 발견 시 해당 사용자에게 즉시 삭제명령 및 확인한 후 구두

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

경고 한다.

② 2회 이상 위반 시 보안규정의 항목에 따라 처리하도록 한다.

3.9.5 예외 및 필요 소프트웨어 신청 절차

① 기본적으로 회사에서 관리하고 있는 소프트웨어 외에 및 필요 소프트웨어는 사용신청서를 작성하여 기술보안담당자에게 제출한다.

② 정보보안그룹에서는 신청 소프트웨어의 업무 연관성, 라이선스 합법성 여부를 판단 후 승인여부를 사용자에게 통보한다.

③ 승인 완료된 소프트웨어는 인가 소프트웨어에 목록에 등재하여 관리하도록 한다.

3.10 보안패치 운영 절차

3.10.1 보안패치 범위

① 보안패치는 운영체제를 사용하는 모든 장비를 대상으로 한다.

② 보안패치의 범위는 운영체제, 응용프로그램 등 업데이트가 가능한 시스템에 적용한다.

3.10.2 유형별 보안패치 적용 방법

① 서버

a. 서버의 보안패치는 운영체제, 응용프로그램은 해당 옵션 설정에서 수동으로 설정한다.

b. 서버의 경우 일 1회 점검하여 수동으로 업데이트를 확인하여 보안패치가 있으면 다운로드를 진행하고 패치 후 관련서버 업무 시스템 담당자와 협의 후 시스템 재부팅을 실행한다.

c. 서버 재시작 후 업무시스템 서비스가 정상적으로 동작하는지 테스트한다.

d. 재부팅이 필요치 않는 보안패치라 하더라도 업무시스템 정상 동작 여부를 반드시 확인하여야 한다.

3.10.3 PC

① 사용자 PC의 보안패치는 운영체제, 응용프로그램은 업데이트 설정에서 자동으로 설정한다.

② 보안패치 설치 후 기존 업무 시스템 및 대외 업무시스템 접속을 통하여 정상적으로 사용가능한 상태인지 반드시 확인한다.

③ 보안패치 후 업무 시스템의 문제가 발생할 경우 즉시 기술보안담당자에게 알리고 조치를 받는다.

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.

3.10.4 방화벽, 공유기, 프린터 등 기타 주변장치

① 방화벽이나 공유기, 프린터 같은 주변기기는 수시로 점검하여 제조사의 보안패치 공지나 수동으로 업데이이트 등을 확인하여 적용하도록 한다.

3.10.5 업무 영양도 분석

① 보안패치를 적용하기전에 패치할 내용을 확인한 후 패치 전과 후 예상되는 변경사항이나 문제점 등을 도출한 후 미리 대응할 수 있도록 대비를 해야한다.

② 보안패치 실행 전 업무 시스템의 영향을 줄 수 있는 경우가 예상이 된다면 사용자에게 사전공지를 하고 변경내용에 대한 교육을 실시한다.

3.10.6 모니터링

① 기술보안담당자는 보안패치 현황을 서버, PC, 기타주변장치등으로 분리하여 관리하도록 한다.

② 기술보안담당자는 보안패치가 정상 동작하는지 불시에 점검하고 패치관련 문제가 발생하면 즉각 지원해야한다.

본 문서의 사용, 배포 등 모든 권리는 정보보안그룹에 있습니다.