# 정보보안 관리규정

GENERAL MANAGEMENT SYSTEM PROCEDURE

| | |
|---|---|
| 문서번호 | IMS-2711-00 |
| 개정차수 | 2 |
| 제/개정일자 | 2021.07.20 |
| 문서구분 | ☐ 관리본 ☑ 비관리본 |
| 관리번호 | n/a (표준기안용) |

**(주)인터비즈시스템**

서울시 강서구 화곡로 416, 16층 (등촌동, 더 스카이밸리5차)
Tel 02-799-7900 / Fax 02-786-0075
http://www.inter-biz.co.kr ㅋ

# 0 제/개정 이력

| 일자 | 개정차수 | 내용 |
|---|---|---|
| 2010년 06월 01일 | 0 | 신규제정 |
| 2021년 05월 18일 | 1 | 전면개정 |
| 2021년 07월 20일 | 2 | 사무실 이전으로 인한 주소 변경 |

공 백

## 1. 적용대상과 범위

이 규정은 (주)인터비즈시스템(이하 "회사"라 한다)의 정보자산을 사용하는 정보시스템 및 구성원에 대하여 적용한다. 단, 회사가 정보자산 보호와 정보운영환경 및 응용프로그램의 운영과 제공에 등에 관하여 별도로 규정한 경우 제외한다.

## 2. 목적

이 규정은 회사의 정보자산을 이용하는 내/외부의 사용자(이하 "사용자"라 한다)에 의해 불법 유출, 파괴, 변경되는 것으로부터 안전하게 보호하며, 네트워크, 정보시스템 및 데이터베이스를 포함한 정보운영환경과 응용프로그램을 보다 안전하고 신뢰성 있게 운영하여 회사 정보자산 이용자에게 원활한 서비스를 제공하도록 하는데 그 목적이 있다

## 3. 의무와 책임

사용자는 이 규정을 준수할 의무가 있으며, 이 규정을 준수하지 않아 발생한 사고의 책임은 원칙적으로 사용자 본인에게 있다.

## 4. 용어의 정의

a) "정보보안"이란 정보처리 수단으로 수집. 가공. 저장. 검색. 송수신 되는 정보의 유출. 위변조. 훼손 등을 방지하거나 정보자산을 보호하기 위하여 관리적. 물리적. 기술적 수단을 강구하는 일체의 행위를 말한다.
b) "정보시스템"이란 PC · 서버 등 단말기, 보조기억매체, 전산 · 통신장치, 정보통신기기, 응용프로그램 등 정보의 수집 · 가공 · 저장 · 검색 · 송신 · 수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
c) "통합전산시스템"이란 인사, 근태, 급여, 교육, 예산, 회계, 구매/계약 등의 업무를 수행하는 ERP시스템과 전자문서에 대한 생산 · 접수 등의 전자결재 업무를 수행하는 그룹웨어시스템을 통칭한다.
d) "업무모듈"이란 ERP시스템을 구성하는 하부 단위업무프로그램을 말한다.
e) "전자문서"란 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송. 수신 또는 저장되는 정보를 말한다.
f) "전자기록물"이란 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송. 수신 또는 저장되는 기록정보자료를 말한다.
g) "전자정보"란 회사에서 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
h) "전산서버실"(이하 "서버실"이라 한다)이란 서버. 네트워크 장비. 백업 장비 등의 전산장비를 설치 운영하고, 전자정보를 운영. 관리하는 실을 말한다.
i) "휴대용 저장매체"란 디스켓 · CD · 외장형 하드디스크 · USB메모리 등 정보를 저장할 수 있는 것으로 PC등의 정보시스템과 분리할 수 있는 기억장치를 말한다.

j) “사용자”란 회사 업무를 수행하기 위해 통합전산시스템에 사용자 등록된 자를 말한다.
k) “CMOS”란 컴퓨터 이용을 위해 장착된 각종 하드웨어의 사용 여부 등 제어에 대한 설정을 말한다.
l) 이 규정에서 정의되지 않은 용어의 정의는 일반적인 전산용어 정의에 따른다.

# 5. 정보보안 담당자 등 지정

## 5.1 정보보안 담당부서와 정보보안담당관 지정

회사의 정보보안담당부서는 경영관리부로 한다
정보보안담당관은 경영지원팀장으로 하며, 다음 각 호의 업무를 수행한다.

a) 정보보안 정책 및 기본계획의 수립 · 시행
b) 정보보안담당자 및 시스템관리자의 업무 관리 감독
c) 정보보안사고 예방 및 사고 조사 결과 처리
d) 사이버 공격 초동조치 및 대응
e) 서버실, 정보시스템 및 정보자료 등의 보안관리
f) 보안심사위원회에 정보보안 분야 안건 심의 주관
g) 정보보안 관리실태 평가 및 심사 분석
h) 정보보안 교육 및 정보협력
i) 주요 정보시스템 기반시설 보호활동
j) ‘사이버보안진단의 날’ 계획 수립
k) 기타 정보시스템 보안관련 활동

## 5.2 정보보안담당자

정보보안담당관은 정보보안담당자를 지정한다.
정보보안담당자는 다음 각 호의 업무를 포함하여 정보보안업무의 실무를 담당한다.

a) 시스템관리자 및 사용자의 정보보안 관련 활동 관리 감독
b) 정보시스템 및 전자정보의 관리, 정보보안, 정보처리실태 점검 및 감독
c) 업무 수행과정에서 발생한 정보보안 관련 문제를 정보보안담당관에게 보고
d) 정보시스템 장비 구매 또는 신규개발 또는 수정변경을 위한 용역 신청
e) 정보자산에 대한 관리

## 5.3 시스템관리자

시스템 관리자는 회사의 정보시스템을 운영, 유지보수 하는 자로 한다.
시스템관리자는 다음 각 호의 업무를 수행한다.

a) 정보침해사고나 시스템 장애 발생시 정보보안담당자 및 정보보안 담당관에게 보고

b) 주요 데이터의 관리기준 및 절차를 수립 · 시행
c) 시스템 장애 및 정전 등으로 부터 정보보호를 위한 주기적인 데이터 백업 시행
d) 정보시스템의 신규개발 또는 수정변경
e) 정보시스템의 유지 · 보수 관리
f) 정보시스템 장비의 반입, 반출 관리
g) 서버실의 출입 관리
h) 사용자 등록, 취소, 제한 등 관리
i) 기타 정보보안담당관이 지정하는 업무

# 6. 정보보안관리

## 6.1 기본수칙

a) 사용자는 개인별 사용자 계정 및 패스워드의 기밀을 유지해야 하며, 본래의 발급 목적으로만 사용하여야 한다.
b) 사용자는 허가받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만 사용할 수 있다.
c) 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 아니 된다.
d) 제C항의 규정에 언급된 행위를 한 사람이 발생될 경우에는 정보보호담당관 및 정보보호담당자에게 즉시 알려야 한다.
e) 사용자는 정보 자산과 연관된 저작권.특허권 및 소프트웨어 라이센스의 사용 조건을 숙지하고 이를 준수하여야 한다.
f) 회사 네트워크시스템을 신설.변경 및 폐기하고자 하는 경우에는 정보보안담당관의 사전승인을 얻어야 한다.
g) 외부 네트워크에서 내부 네트워크로의 접근은 회사에서 승인한 정보시스템을 제외하고는 원칙적으로 허용하지 아니한다. 단, 필요시 적법한 절차에 의해 요청하여 승인된 경우에 한하여 제한적으로 허용될 수 있다.
h) 사용자는 업무와 관련하여 습득한 정보자산을 회사의 허가 없이 외부에 누출해서는 아니된다.
i) 정보보안 사고의 책임은 원칙적으로 사용자 본인에게 있다.

## 6.2 대외비

정보보안담당관은 다음 각 호에 해당하는 사항을 대외비로 관리하여야 한다

a) 정보통신망 세부 구성현황(IP 세부 할당현황 포함)
b) 정보통신망 보안취약점 분석 · 평가 결과물
c) 그 밖에 보호할 필요가 있는 정보통신망 관련 자료

## 6.3 정보보안점검

정보보안 점검 시 대상 및 분야를 해당 부서에 통보하며, 해당 부서에서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비하고 관련 사용자는 정보보안점검에 적극 협조하여야 한다.

정보보안 점검 실시 결과를 해당 부서에 통보하며 해당 부서에서는 지적사항을 즉각 시정하고 시정 결과를 회신하여야 한다.

## 6.4. 사이버보안 진단의 날

a) 정보보안담당자는 매월 셋째 수요일을 “사이버보안 진단의 날”로 지정하여 운용하여야 한다
b) 정보보안담당자는 “사이버보안 진단의 날”을 이용하여 정보시스템의 악성코드 감염여부, 보안 취약여부 등 정보보안업무 전반에 대하여 체계적이고 종합적인 보안진단을 실시하여야 한다.
c) 정보보안담당자는 “사이버보안 진단의 날”에 정보시스템 대상으로 악성코드 감염여부와 정보시스템의 보안 취약여부 등을 진단하여 문제점을 발굴 개선하여야 한다.
d) 정보보안담당자는 제b항에 따른 보안진단 결과를 정보보안담당관에게 보고하여야 한다.
e) 회사 전 직원은 “사이버보안 진단의 날”에 pc진단프로그램, 휴대용저장매체관리 프로그램, USB자동실행 차단프로그램 실행 등 제반 정보보안강화 조치를 하여야 한다.

## 6.5 정보자산의 이동 통제

a) 정보자산은 정보보안담당자의 허가 없이 옮겨져서는 아니 된다.
b) 정보자산은 이동 시 기밀성, 무결성, 가용성이 최대한 유지되도록 적절한 방법에 의해 통제되어야 하며, 정보자산의 이동은 반드시 정보보안담당자의 승인을 받아야 한다.
c) 정보보안담당자는 정보자산의 이동 등 변경사항에 대해 기록하여야 한다.

## 6.6 정보보안 교육

a) 정보보안담당관은 사용자를 대상으로 정보보안 교육을 실시하여 정보보안에 대한 인식을 제고하고 사용자와 시스템 관리자의 부주의나 고의에 의한 정보보안 사고를 최소화하여야 한다.
b) 정보보안 교육은 대상별로 실시할 수 있으며, 필요에 따라 연 1회 이상 수시로 실시한다.

## 6.7 인적보안

a) 정보보안담당관은 직원의 휴직 또는 퇴직 발령 시 인사 대상자에 대한 계정 및 공용계정에 대한 접근 권한을 즉시 제거한다.
b) 정보보안담당관은 직원 입사시 보안서약서(별지 제1호 서식)를 수령하여 보관한다.
c) 정보보안담당관은 정보시스템 및 관련 기반시설의 관리 운영을 외부에 위탁할 때에는 계약서에 정보보안관련 사항(별표1 및 별표2)을 반영한다.

## 6.8 침해사고 대응

a) 정보보안담당관은 회사 정보시스템의 비 인가된 접근, 오남용(비 인가된 사용) 및 해킹사고뿐만 아니라 바이러스 사고 등의 침해사고시를 대비하여 비상연락체계를 갖추고 대응계획을 수립한다.
b) 비상연락체계의 구성과 임무에 대해서는 정보보안담당관이 따로 정한다.

## 6.9 원격근무 보안관리

정보보안담당관은 재택, 파견 및 출장 등 원격근무를 지원하기 위한 정보시스템을 도입, 운영할 경우 관리적 · 물리적 · 기술적 보안대책을 수립 시행하여야 한다.

정보보안담당관은 원격근무 가능업무 및 공개 · 비공개 업무 선정기준을 수립하되 대외비 이상 비밀자료를 취급하는 업무를 원격근무 대상에서 제외한다.

원격근무자는 원격근무에 대한 'SSL VPN 사용계정 요청'을 문서로 신청하여야 하며, 다음 각 호를 준수하여야 한다.

a) 부여받은 인증관련 정보 및 매체를 타인에게 유출하지 않는다.
b) 원격근무 중 작성 · 저장 · 열람 · 출력한 문서는 업무목적에만 활용하고 타인에게 유출하지 않는다.
c) 원격근무용 소프트웨어 및 전산장비를 업무목적에만 활용하며 바이러스 백신 프로그램 및 기타 보안 프로그램을 설치하여 최신상태로 유지한다.

## 6.10 바이러스 예방 및 조치

시스템관리자는 컴퓨터 바이러스, 웜 발생 등으로 심각한 피해가 우려되는 경우 게시판이나 메일 등을 통하여 경고 메시지 게시 등의 조치를 취한다.

시스템관리자는 무단, 불법 복사된 프로그램을 설치한 정보시스템의 회사 전산망 접속을 제한한다.

사용자는 바이러스, 웜 감염을 예방하기 위하여 다음과 같이 조치하여야 한다.

a) 시스템관리자가 인증한 바이러스 백신 프로그램 설치 및 최신 버전 유지
b) 주기적인 보안패치 적용
c) 주기적인 바이러스 검사 및 외부 저장매체 보관, 파일. 인터넷 다운로드, 파일. 외부 전송, 메일의 첨부파일 실행 또는 열기 전 바이러스 검사 실시
d) 정기적인 중요 데이터 백업
e) 무단, 불법 복사된 프로그램 설치 금지 및 검증되지 않은 프리웨어 다운로드 지양
f) 수신인이 불분명한 메일의 확인 금지
g) 기타 필요한 정보보안 조치

바이러스의 감염이 의심될 경우 사용자는 즉각 네트워크 접속을 단절시킨 후 시스템관리자에게 통보한다.

시스템관리자는 바이러스의 감염이 확인된 경우 정보보안담당관에게 보고해야 하고, 정보보안담당관은 침해사고 계획에 다라 대응한다.

### 6.11 부적절한 사용 및 제재

사용자는 정보시스템 사용에 있어 적절성을 유지하여야 하며, 각 호에 해당하는 경우에는 부적절한 사용으로 간주하여 제재할 수 있다.

a) 타 사용자의 계정 및 패스워드를 허가 없이 사용한 경우
b) 타 사용자의 정당한 사용을 방해한 경우
c) 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 경우
d) 사용자가 시스템관리자 및 데이터베이스관리자의 패스워드 또는 타 사용자의 패스워드를 획득하고자 해킹하는 경우
e) 개인정보파일 등 중요 전자정보를 불법으로 외부에 유출한 경우
f) 외부의 불법사용자에게 계정 및 패스워드를 제공한 경우
g) 시스템관리자가 특별한 사유 없이 패스워드를 사용자와 공유한 경우
h) 정보시스템을 통해 음란 사이트 등 반사회적인 유해사이트를 접속. 개설. 열람하는 경우
i) 개인의 이익이나 상업적 목적으로 스팸메일을 발송하는 경우
j) 무단, 불법 복사된 프로그램을 설치하여 사용하거나 금지된 프리웨어를 사용한 경우
k) 보안 점검의 지적사항에 대하여 즉각적인 시정을 취하지 않는 경우

부적절한 사용에 의하여 회사에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각 호의 제재 조치를 취할 수 있으며, 구체적인 사항은 보안심사위원회에서 심의한다.

a) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의한 법적조치
b) 회사 「인사규정」에 의한 징계조치
c) 사용자의 정보시스템 사용 제한 또는 금지, 사용자 계정 회수 · 삭제

## 6.12 전자우편 보안대책

a) 정보보안담당관은 웜 · 바이러스 등 악성코드로부터 사용자PC등 전자우편 시스템 일체를 보호하기 이하여 국가정보원장이 안전성을 확인한 백신, 바이러스 월, 해킹메일 차단시스템을 구축하는 등 보안대책을 강구하여야 한다.
b) 사용자는 전자우편으로 업무자료 송수신시 기관의 전자우편을 사용하여야 하며, 상용 전자우편 사용을 불허한다.
c) 사용자는 메일에 포함된 첨부파일이 자동 실행되지 않도록 설정하고 첨부파일 다운로드 시 반드시 최신 백신으로 악성코드를 검사하여야 한다.
d) 사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람하지 않아야 하고, 해킹메일로 의심되는 메일 수신시에는 즉시 정보보안담당관에게 신고하여야 한다.

## 6.13 휴대용 저장매체

a) 정보보안담당관은 휴대용 저장매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위변조, 훼손, 분실 등에 대비한 보안대책을 강구하여야 한다.
b) 정보보안담당관은 휴대용 저장매체를 비밀용, 일반용으로 구분하고 휴대용 저장매체 관리대장(별지 제3호 서식)을 작성 · 관리하여 주기적으로 수량 및 보관 상태를 점검하여 반출 · 입을 통제하여야 한다.
c) 정보보안담당관은 USB관리시스템을 도입할 경우 국가정보원장이 안정성을 확인한 제품을 도입하여야 한다.
d) 정보보안담당관은 사용자가 USB메모리를 PC등에 연결 시 자동 실행되지 않도록 하고 최신 백신으로 악성코드 감염여부를 자동 검사하도록 설정하여야 한다.
e) 비밀자료가 저장된 휴대용 저장매체는 매체별로 비밀등급 및 관리번호를 부여하고, 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다.
f) 휴대용 저장매체를 파기 등 불용처리 하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우 저장되어 있는 정보의 복구가 불가능하도록 완전삭제 프로그램을 사용하여야 한다.
g) 정보보안담당관은 사용자의 휴대용 저장매체 무단 반출 및 미등록 휴대용 저장매체 사용 여부 등 보안관리 실태를 주기적으로 점검하여야 한다.
h) 그 밖에 휴대용 저장매체의 보안관리에 관련된 사항은 'USB 메모리 등 휴대용 저장매체 보안관리지침'을 따른다.

## 6.14 전자정보 저장매체 불용처리

a) 정보보안담당관은 전자정보 저장매체를 불용처리(교체 · 반납 · 양여 · 폐기 등)하는 경우 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.
b) 자료의 삭제 시에는 해당 정보가 복구될 수 없도록 삭제방법을 적용하여야 한다.

### 6.15 사용자 고지

정보보안담당관은 제6.10조 제1항의 상황이 발생하였을 때에는 그 사실을 사용자에게 고지하여야 한다. 다만, 사용자에게 경미한 영향을 미치거나, 신속히 처리해야 하는 등의 긴급한 상황일 경우에는 고지하지 아니할 수 있다.

### 6.16 사용자 구제조치

정보보안담당관은 사용자의 불만사항 및 침해사고 피해발생시 처리절차 등을 게시판 등에 고지하여야 한다.

## 7. 서버실 운영 및 관리

### 7.1 서버실 기능

회사의 서버실 및 정보시스템 운영 · 관리를 위한 서버실 기능은 다음 각 호와 같다.

a) 전산망 구축 및 각종 전산장비 운영. 관리
b) 정보활동에 필요한 자료의 수집. 정리. 운영. 관리

### 7.2 서버실 운영 · 관리 부서 및 시스템관리자

서버실 운영 · 관리부서는 경영관리부로 하며, 운영관리담당자는 시스템관리자로 한다.

### 7.3 출입관리 및 통제

서버실은 통제구역으로 설정하여 비인가자의 출입을 통제한다.

다음 각 호의 사유로 서버실에 출입하고자 하는 자는 '서버실 출입신청서(별지 제4호 서식)'를 작성하여 시스템관리자 및 정보보안담당자의 승인을 받은 후, 서버실 입구에 비치된 '서버실 출입 관리대장'에 출입시간 및 출입목적 등을 기록하여야 하며, 시스템관리자는 출입자와 동반입회 하여야 한다.

a) 정보시스템 설치, 점검 등 작업과 관련하여 출입하고자 하는 사람
b) 장애처리 등 정보시스템 운영과 관련하여 출입하고자 하는 사람
c) 기타 업무와 관련하여 서버실을 출입하고자 하는 사람

시스템관리자는 다음 각호에 해당되는 자의 서버실 출입을 금지한다.

a) 출입절차를 이행하지 않은 사람
b) 음주 등 행동의 제약을 받는 행위를 한 사람
c) 서버실 반입금지 물품을 소지한 사람
d) 기타 출입에 제한이 필요하다고 인정되는 사람

### 7.3 장비 반출입 관리

장비 반출입을 원하는 사람은 '장비 반입·반출 신청(승인)서(별지 제5호 서식)' 를 작성하여 반출입 내역 및 목적등을 명확히 하여야 하며, 시스템관리자는 다음 각 호에 해당되는 장비에 대하여 반출입을 승인할 수 있으며, '장비 반출입 관리대장' 에 반출입 내역 및 반출입 목적 등을 기록관리 하여야 한다.

a) 신규(증설) 설치, 교체, 수리, 폐기를 위한 장비
b) 장애처리, 유지보수를 위해 필요한 장비 및 각종 부품
c) 전기, 통신, 공조, 소방 등 부대설비
d) 기타 서버실 운영관리에 필요한 기기 등

다음 각 호에 해당되는 물품은 서버실 반입을 금지한다.

a) 총검, 폭발물, 화약 등 위험물
b) 해머, 망치 등 파괴 가능한 공구류
c) 신경가스 등 화학류
d) 라이터, 신나, 물 등 인화 및 액체류
e) 기타 정보시스템에 유해 가능성이 있는 물품

## 8. 서버시스템 및 데이터베이스 관리

### 8.1 운영 및 관리

서버시스템 및 데이터베이스(이하 본장에서 '서버시스템 등' 이라한다)는 경영관리부에서 관리하며, 서버시스템 등의 관리자는 전산실장으로 한다. 다만, 자체 서버시스템 등을 운영하고 있는 부서는 해당 부서의 장이 자체 운영 서버시스템의 관리자가 된다.

서버시스템 등의 관리자는 사용자의 패스워드를 확인해 해킹 위험이 있는 단순한 조합의 패스워드로 판단되는 경우 당사자에게 통보하여 변경을 요구할 수 있다.

서버시스템 등의 관리자는 데이터베이스에 대한 모든 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

### 8.2 계정관리

서버시스템 등의 운영 관리자는 다음 각 호와 같이 계정을 관리하여야 한다.

a) 사용자별 또는 그룹별로 접근권한을 부여한다.
b) 사용자 계정의 등록.변경 및 폐기는 시스템관리자가 실시하며, 특별한 상황이 발생하는 경우에 한하여 부서장의 허가를 받은 후 작업을 실시한다.
c) 외부 사용자의 계정은 유효기간을 설정한다.

d) 일정 횟수 접속 실패 시 사용을 금지한다.
e) 특정 단말에서만 슈퍼유저의 접속을 허용한다.

# 9. 네트워크 시스템 관리

## 9.1 네트워크 시스템 관리

a) 네트워크 시스템은 경영관리부에서 통합 관리하며, 관리자는 전산실장으로 한다.
b) 사용자는 임의로 네트워크 IP주소를 변경할 수 없다.
c) 인터넷을 이용한 모든 외부로부터의 접근은 원칙적으로 방화벽을 통해서만 접근할 수 있도록 한다.
d) 외부접속자의 관리자 로그인은 허용하지 아니한다. 다만, 회사 네트워크를 유지보수하는 업체의 원격 관리자 로그인은 허용한다. 이 경우 정보보안담당자는 원격 관리자의 명단을 유지하고 '보안 및 비밀유지각서(별지 제2호 서식)'를 받아야 한다.

## 9.2 네트워크 시스템 보호

a) 정보보안담당관은 회사에 유해하거나 불필요하다고 판단되는 웹사이트의 접속을 통제할 수 있으며, 사용자가 회사 정보보안 기대수준에 미달하는 경우 네트워크 사용을 제한할 수 있다.
b) 정보보안담당관은 의심스러운 활동에 대해서는 방화벽, 침입탐지시스템 및 기타 보안 시스템의 로그를 분석하여 해당 내용을 확인하여야 하고, 네트워크 관리 정책에 대한 변경관리를 하여야 한다.
c) 사용자는 회사 네트워크 사용 시 적법한 사용자임을 인증받고 사용자의 PC. 응용프로그램 등의 무결성 수준 및 보안수준을 점검하여야 한다.

# 10. 통합전산시스템

## 10.1 통합전산시스템 사용자 계정 발급 및 폐기 기준

a) 신규 입사자는 통합전산시스템에 등록 후 사용자 계정이 발급된 시점부터 통합전산시스템을 사용할 수 있으며, 사용자 계정은 퇴직 시까지 사용된다.
b) 퇴사자는 통합전산시스템에 퇴직 처리되는 시점부터 통합전산시스템을 사용할 수 없도록 조치할 수 있다.

### 10.2 사용권한 부여 및 제한

경영관리부에서 사용자 직위, 담당업무에 따라 통합전산시스템 업무모듈의 사용권한을 이용대상에게 부여한다.

### 10.3 사용권한 요청 및 허가절차

a) 신규로 해당분야의 전자문서 이관이 필요한 경우 협조문으로서 경영관리부에 요청을 한다.
b) 인사 이동에 의한 사용권한 변경은 별도의 요청 없이 경영관리부에서 처리한다.

### 10.4 메일계정 발급 및 삭제기준

경영관리부는 통합전산시스템에 사용자 등록된 인원에 메일계정을 발급한다.

제1항에 해당하지 않는 자가 메일계정을 요청하는 경우, 계정의 발급을 경영관리부에 문서로써 요청하여야 하며 정보보안담당관은 이를 결정한다.

정보보안담당관은 다음 각 호의 어느 하나에 해당하는 사항에 대해서 해당 메일계정을 삭제할 수 있다.

a) 타인의 메일 계정을 도용하거나 부정하게 사용한 경우
b) 불특정 다수 및 타인에게 피해를 주거나 미풍양속을 해치는 행위를 한 경우
c) 서비스 운영을 고의로 방해한 경우

## 11. 사용자

### 11.1 PC 관리

사용자는 업무용 PC(노트북, 넷북 등 유사 정보시스템 포함)를 사용에 있어 보안의 적절성을 유지하여야 하며, 다음 각 호가 지켜지지 않을 시에는 부적절한 사용으로 간주하여 제재조치할 수 있다.

a) PC 기동시 CMOS 및 PC운영체제에서 제공하는 패스워드 설정
b) 10분 이상 자리 비울 시 화면보호기 작동 및 패스워드를 설정, 장시간자리를 비울 시 전원 오프 설정
c) 응용 프로그램의 무단복사 금지
d) 이동식 저장매체를 사용 및 네트워크를 이용하여 전자정보 전송시 패스워드를 설정 및 바이러스 검사
e) 중요한 데이터 파일(개인정보 등)암호화 및 패스워드를 설정

11.2 계정 관리

사용자는 업무용 PC(노트북, 넷북 등 유사 정보시스템 포함)에서 사용하는 자신의 계정 및 패스워드가 외부로 노출되지 않도록 유의하고, 주기적으로 이를 변경하여야 한다.

## 11.3 바이러스 주의

a) 사용자는 발송자를 확인할 수 없는 전자우편 또는 제공자가 불확실한 컴퓨터프로그램 등에 대해 안전성여부를 확인하고 실행하여야 한다.
b) 사용자는 컴퓨터바이러스 방지프로그램을 설치하여 침투여부를 수시로 점검하고, 침투한 경우에는 이를 제거 · 복구하여야 한다.
c) 사용자는 최신의 윈도우 업데이트를 주기적으로 실행하며 필요한 보안패치를 반드시 적용하여야 한다.

## 11.4 PC 폐기

a) 사용자는 PC의 폐기 시에는 반드시 저장장치를 분리하여 별도 파기하거나 초기화 한다.
b) 정보보안담당관은 사용자정보, 중요 컨텐츠 등 민감한 내용이 보관된 PC의 경우 PC 폐기 처리결과에 대해 사후검토를 실시할 수 있다.

## 11.5 불법소프트웨어에 대한 책임

a) 불법소프트웨어의 사용에 대한 책임은 사용자 및 사용자 소속부서의 팀장에게 있다.
b) 각 팀장은 구성원이 불법소프트웨어를 사용하지 않도록 관리감독을 하여야 한다.

## 11.6 사이버 보안 진단 수행

a) 정보보안담당자가 매월 셋째 주 수요일에 실시하는 사이버 보안진단의 날의 시행에 사용자는 협조해야 한다.
b) 정보보안담당자가 지정한 지정된 정보보호 소프트웨어를 사용하여 사이버 보안진단을 수행해야 하며 이상이 있을시 그 결과를 정보보안담당관에게 통보하여야 한다.
c) 정보보안담당자는 사이버 보안진단을 수행하지 않는 사용자의 전산망 접속을 제한할 수 있다.

# 12. 보칙

## 12.1 준용

이 규정이 정하는 바 이외의 정보보호업무에 관한 사항은 다음 관계 법령과 회사의 제반규정에 따른다.

a) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
b) 「개인정보 보호법」

# 13. 기록 및 보관

| 양식번호 | 양 식 명 | 보관기간 | 보존년한 | 비고 |
|---|---|---|---|---|
| IBF-2711-00-01 | 정보보안 서약서 | 3년 | 5년 | |

[별표 1]

## 사업자 보안위규 처리기준

| 구 분 | 위 규 사 항 | 처 리 기 준 |
|---|---|---|
| 심각 | 1. 비밀 및 대외비 급 정보 유출 및 유출시도<br>가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 유출<br>나. 개인정보 · 신상정보목록 유출<br>다. 비공개 항공사진 · 공간정보등 비공개 정보 유출<br>2. 정보시스템에 대한 불법적 행위<br>가. 관련 시스템에 대한 해킹 및 해킹시도<br>나. 시스템 구축 결과물에 대한 외부 유출<br>다. 시스템 내 인위적인 악성코드 유포 | ◦ 사업참여 제한<br>◦ 위규자 및 직속 감독자 등 중징계<br>◦ 재발방지를 위한 조치계획 제출<br>◦ 위규자 대상 특별 보안교육 실시 |
| 중대 | 1. 비공개 정보 관리 소홀<br>가. 비공개 정보를 책상 위 등에 방치<br>나. 비공개 정보를 휴지통·폐지함 등에 유기 또는 이면지 활용<br>다. 개인정보, 신상정보 목록을 책상 위 등에 방치<br>라. 기타 비공개 정보에 대한 관리소홀<br>2. 사무실·보호구역 보안관리 허술<br>가. 통제구역 출입문을 개방한 채 퇴근 등<br>나. 인가되지 않은 작업자의 내부 시스템 접근<br>다. 통제구역 내 장비 · 시설등 무단 사진촬영<br>3. 전산정보 보호대책 부실<br>가. 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반<br>나. 웹하드 ·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신<br>다. 개발 · 유지보수시 원격작업 사용<br>라. 저장된 비공개 정보 패스워드 미부여<br>마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장<br>바. 외부용 PC를 업무망에 무단 연결 사용<br>사. 보안관련 프로그램 강제 삭제<br>아. 사용자계정관리 미흡 및 오남용(시스템 불법접근시도 등) | ◦ 위규자 및 직속 감독자 등 중징계<br>◦ 재발방지를 위한 조치계획 제출<br>◦ 위규자 대상 특별 보안교육 실시 |

| 구 분 | 위 규 사 항 | 처 리 기 준 |
|---|---|---|
| 보통 | 1. 기관 제공 중요정책·민감 자료 관리 소홀<br>가. 주요 현안·보고자료를 책상 위 등에 방치<br>나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용<br>2. 사무실 보안관리 부실<br>가. 캐비넷·서류함·책상 등을 개방한 채 퇴근<br>나. 출입키를 책상 위 등에 방치<br>3. 보호구역 관리 소홀<br>가. 통제·제한구역 출입문을 개방한 채 근무<br>나. 보호구역내 비인가자 출입허용 등 통제 미실시<br>4. 전산정보 보호대책 부실<br>가. 휴대용저장매체를 서랍·책상 위 등에 방치한 채 퇴근<br>나. 네이트온 등 비인가 메신저 무단 사용<br>다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근<br>라. 부팅·화면보호 패스워드 미부여 또는 "1111" 등 단순숫자 부여<br>마. PC 비밀번호를 모니터 옆 등 외부에 노출<br>바. 비인가 보조기억매체 무단 사용 | ◦ 위규자 및 직속 감독자 등 경징계<br>◦ 위규자 및 직속 감독자 사유서 / 경위서 징구<br>◦ 위규자 대상 특별 보안교육 실시 |
| 경미 | 1. 업무 관련서류 관리 소홀<br>가. 진행 중인 업무자료를 책상 등에 방치, 퇴근<br>나. 복사기·인쇄기 위에 서류 방치<br>2. 근무자 근무상태 불량<br>가. 각종 보안장비 운용 미숙<br>나. 경보·보안장치 작동 불량<br>3. 전산정보 보호대책 부실<br>가. PC내 보안성이 검증되지 않은 프로그램 사용<br>나. 보안관련 소프트웨어의 주기적 점검 위반 | ◦위규자 서면·구두 경고 등 문책<br>◦ 위규자 사유서 / 경위서 징구 |

[별표 2]

## 보안 위규자 행정처리 및 위약금 부과 기준

□ 보안 위규자 행정처리 기준

| 구분 | 위규 수준 | | | |
|---|---|---|---|---|
| | A급 | B급 | C급 | D급 |
| 위규 | 심각 1건 | 중대 1건 | 보통 2건 이상 | 경미 3건 이상 |
| 위약금 비 중 | 부정당업자 등록 | 계약금액의 5% 이하 | 계약금액의 3% 이하 | 계약금액의 1% 이하 |

□ 보안 위약금 부과 기준

* 위규 수준은 [별표 제1호] 참고

1. 보안 위약금은 다른 요인에 의해 상쇄, 삭감이 되지 않도록 부과

* 보안사고는 1회의 사고만으로도 그 파급력이 큰 것을 감안하여 타 항목과 별도 부과

2. 사업 종료 시 지출금액 조정을 통해 위약금 정산

**[별지 제1호 서식]**

# 정보보안 서약서

생 년 월 일
성 명

상기 본인은 본 서약서가 (주)인터비즈시스템(이하 “회사”라 한다) 재직기간뿐만 아니라 퇴직 후에도 적용될 수 있음을 인식하고 회사의 정보보안과 관련 아래의 준수사항에 대하여 서명 전 숙독하였으며 이를 준수할 것을 서약합니다.

- 아 래 –

1. 본인은 직간접적으로 취득한 회사의 영업비밀, 개인신상 정보와 이를 생산, 보관, 유통, 폐기하는 과정에서 사용되는 모든 물리적 매체 및 산출자료(예: 전산장비, 정보정장 및 전송장비, 보고서 등 서류, 사진, 전자파일, 기타 매체와 자료 등)가 회사 소유의 정보자산(이하 “정보자산”이라 한다)임을 확인합니다.

2. 본인은 재직기간 동안 알게 된 정보자산 및 회사 소유의 지적재산권 등을 분실, 훼손, 침해되지 아니하도록 안전하게 사용, 관리하고 보안 관련 사고가 발생하지 않도록 하겠습니다. 그리고 정보자산 및 지적재산권 등을 지정된 업무에 사용할 목적을 제외하고는 회사의 사전 서면동의 없이 반출하거나, 개인적 용도나 제3자를 위한 정보로 이용하지 않겠으며, 자3자에게 누설, 공개, 변조, 복사, 촬영 및 기타 방법에 의한 복제 등의 행위를 일체 하지 않겠습니다.

3. 본인은 정보자산 보호, 유출 방지 및 사회적 물의 또는 불법행위 등의 예방하는 등 정상적인 경영활동을 위하여 필요한 범위 내에서 메일, 인터넷 접속 등 모든 종류의 유, 무선 통신에 의한 음향, 문언, 부호 또는 영상 등에 대하여 회사가 예고 없이 내용을 검색한다는 사실을 인지하고 있으며, 이에 동의합니다.

4. 본인은 회사에서 인가한 정보자산만을 취급하고, 명백히 허가 받지 않은 정보나 시설 또는 장치(데이터베이스서버, 파일서버, 메일서버 등)에 접근하지 않으며 회사 관련 업무를 수행할 때만 회사 시설 또는 장치를 이용하고 이 시설 또는 장치에 사적 정보를 보관하지 않겠습니다. 또한 승인 받지 않은 프로그램, 불법 스프트웨어 및 정보와 인가되지 않는 정보저장매체 등을 회사 내에서 사용하지 않겠으며, 회사가 요구하는 보안 정책을 성실히 따르겠습니다.

5. 본인은 퇴직 시 재직기간 동안 취득한 회사 소유의 정보자산을 반드시 반납 또는 폐기할 것이며, 회사 요청 시 폐기에 대한 증빙자료를 제공하겠습니다. 또한 회사의 사전 서명동의 없이는 이를 개인적으로 유용하거나 공개 또는 제3자에게 누설하는 등의 행위를 하지 않겠습니다.

6. 본인은 거래처 및 고객 소유의 정보자산에 대하여도 회사 소유의 정보자산과 동일한 수준으로 정보 보안을 유지, 관리하겠습니다.

7. 본인은 본인에게 부여된 사용자 ID, 비밀번호 등을 타인과 공동사용 또는 누설치 않겠습니다.

상기 사항을 숙지하고 이를 성실히 준수할 것을 동의하며, 본 서약서의 준수사항을 위반할 경우에는 “부정경쟁방지 및 영업비밀에 관한 법률”, “정보통신망이용촉진 및 정보보호 등에 관한 법률” 등 관련 법령에 의한 일체의 민형사상 책임 이외에도 회사 관련 규정에 따른 징계조치 등 어떠한 불이익도 감수할 것이며, 회사에 끼친 손해에 대해 지체 없이 변상 또는 복구 할 것을 서약합니다.

본 서약과 관련 분쟁이 발생하는 경우, 회사 소재의 관할법원에서 분쟁을 해결하는데 동의합니다.

_____년 ____월 ____일

서 약 자: _____ (인)

**(주) 인터비즈시스템 귀중**

**[별지 제2호 서식]**

# 보안 및 비밀유지각서

본인은 인터비즈시스템(이하 “회사”)에서 용역을 수행함에 있어 다음사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 “회사”에서 “용역” 수행중 취득한 제반 비밀사항을 업무 수행중은 물론 복귀 후에도 일체 누설하지 않을 것을 서약합니다.

2. 본인은 “회사”의 기밀을 누설하였을 때는 동기여하를 막론하고 그 결과에 대한 제반 법규에 의거하여 엄중한 처벌을 받을 것을 서약 합니다.

3. 본인은 업무상 고의 또는 중대 과실로 인해 “회사”에 재산상 손해를 끼쳤을 경우에 그에 대한 형사 및 민사상 책임을 집니다.

21 년 월 일

서약자 소속 :

소속회사주소 :

근 무 기 간 :

전 화 번 호 :

성 명 : (인)

[별지 제3호 서식]

# 휴대용 저장매체 관리대장

관리 담당자 :

| 연번 | 관리번호(S/N) | 매체 구분 | 등록일자 | 사용자명 | 불용처리일자 | 불용처리방법 (재사용용도) | 비고 |
|---|---|---|---|---|---|---|---|
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |
| 7 | | | | | | | |
| 8 | | | | | | | |
| 9 | | | | | | | |
| 10 | | | | | | | |
| 11 | | | | | | | |
| 12 | | | | | | | |
| 13 | | | | | | | |
| 14 | | | | | | | |
| 15 | | | | | | | |
| 16 | | | | | | | |
| 17 | | | | | | | |
| 18 | | | | | | | |
| 19 | | | | | | | |
| 20 | | | | | | | |

**[별지 제4호 서식]**

# 서버실 출입신청서

| | | | |
|---|---|---|---|
| 신 청 자 | | 소 속 | |
| 업 체 | | 연 락 처 | |
| 출입일자 | | 입실시간 | |
| | | 퇴실시간 | |
| 출입목적 | □장애처리 □작업 □견학 및 방문 □점검 □기타( ) | | |
| 작업내역 | | | |
| 특이사항 | | | |
| 출입인원 | ※ 다수인원 출입시 별도 첨부 | | |

위 목적으로 전산서버실 출입을 신청합니다.

년 월 일

신청인 (인)

전산서버실 출입을 승인합니다.

년 월 일

시스템관리자 (인)

[별지 제5호 서식]

# 장비 반입 · 반출 신청(승인)서

| | | | | |
|---|---|---|---|---|
| 신청인 | 성 명 | | 생년월일 | |
| | 소 속 | | 기 타 | |
| | 주 소 | | 연락처 | TEL<br>H.P |
| | 반입. 출 일시 | | 반입. 출 사유<br>(관련 공문) | |
| | 반입. 출 장소 | | | |

| | 품 명 | 규 격 ( 모 델 ) | 수 량 | 용 도 | 비 고 |
|---|---|---|---|---|---|
| 물품내역 | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| | | | |
|---|---|---|---|
| 확 인 담 당 자 | ( 인 ) | 연 락 처 | |

위 장비의 (반입 · 반출)을 신청합니다.

년 월 일

위 신 청 인 : ( 인 )

위 조건으로 신청사항을 승인합니다.

년 월 일

정보보안 담당자 ( 인 )

| | |
|---|---|
| ※ 반입. 출 장비 확인 | 일 시 : 년 월 일 |