부현전기	사규	문서번호	BTMS-RH-008
	정보보호규정	개정번호	01
		개정일자	2022-09-30
		페 이 지	

개 정 이 력				관리구분 ■ 관리본 □ 비관리본		□ 비관리본
개정번호	개정일자	개정사유 및 내용	작성	검토 승인		승인
01	2022-09-30	최초 제정	과장 이광훈	진행원		김홍수

# 제 1 장 총 칙

## 제1조(목적)

이 규정은 ㈜부현전기 (이하 "회사"라 한다) 전 임직원의 정보보호 인식과 보안 수준을 제고하고 정보통신망의 안정성과 신뢰성 확보를 위하여 필요한 사항을 정하는 것을 목적으로 한다.

## 제2조(적용범위)

- 1. 이 규정은 회사의 정보자산을 이용하거나 관리하는 회사의 임직원과 회사를 위해 종사하는 외부인에게 모두 적용한다.
- 2. 이 규정은 관리적, 기술적, 물리적 보호가 필요한 회사의 주요 정보 자산을 대상으로 한다.

#### 제3조(용어의 정의)

- 이 규정에서 사용하는 용어는 다음 각 호와 같다.
- 1. 정보보호관리체계

회사의 주요 정보 자산을 보호하기 위한 정보보호 관리 절차와 과정을 체계적으로 수립

하여 지속적으로 관리·운영하기 위한 종합적인 체계를 말한다.

#### 2. 정보보호

"정보보호"란 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신되는 정보의 유출, 위/변조, 훼손 등을 방지하기 위하여 관리적, 물리적, 기술적 수단을 강구하는 일체의 행위를 말한다.

#### 3. 정보 자산

"정보 자산"이란 회사의 모든 정보와 지적 재산권, 특허, 영업비밀 등 기술상 경영상의 내용 그 자체와 이를 포함하고 있는 정보시스템과 정보시스템의 운영·관리에 필요한 시설, 전자정보 등 자원을 총칭한다.

#### 4. 정보보호책임자

- ① 정보보호 업무를 총괄하는 ISO(ISO: Information Security Officer)를 의미한다.
- ② 인사, 총무 관련팀장이 그 역할을 담당한다.

#### 5. 외부인

임직원이 아닌 외부인원으로서 회사와의 계약에 의해 본사에 상주하여 근무하는 인원 및 일시적 방문자를 포함한다.

6. 정보보호관련규정

정보보호와 관련된 사규, 절차서 및 지침서와 관련 법규를 이하 '정보보호관련규정'이라 한다.

## 제 2 장 책임과 권한

#### 제4조(책임과 권한)

- 1. 정보보호책임자(ISO)는 정보보호 업무와 관련하여 다음 각호의 업무를 수행한다.
  - ① 정보보호 계획의 수립·시행 및 개선
  - ② 정보보호 실태와 관행의 정기적인 감사 및 개선
  - ③ 정보보호 위험의 식별 평가 및 정보보호 대책 마련
  - ④ 정보보호 교육과 모의 훈련 계획의 수립 및 시행
  - ⑤ 『정보보호산업의 진행에 관한 법률』 제13조에 따른 정보보호 공시에 관한 업무
  - ⑥ 『개인정보 보호법』제31조 제2항에 따른 개인정보 보호책임자의 업무
  - ⑦ 기타 정보보호를 위하여 필요한 조치의 이행

#### 2. 정보보호 담당부서

- ① 정보보호 담당부서는 정보통신망과 정보시스템의 안전성 및 정보보호관련규정의 준수 여부를 주기적으로 점검하여야 하며 전 임직원과 외부자는 이에 적극 협조하여야 한다.
- ② 정보보호 담당부서는 보안 사고를 예방하기 위한 목적으로 정보보호 점검 활동을 시행할 수 있다.
- 3. 전 임직원과 외부인은 다음 각 호의 정보보호 활동 기본 수칙을 준수하여야 한다.
  - ① 개인별 사용자 계정 및 비밀번호의 기밀을 유지하여야 하며, 본래의 발급 목적으로만 사용하여야 한다.
  - ② 허가 받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만 사용하여야 한다.
  - ③ 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 아니 된다.
  - ④ 정보 자산과 연관된 저작권·특허권 및 소프트웨어 라이선스의 사용 조건을 숙지하고 이를 준수하여야 한다.
  - ⑤ 업무와 관련해 습득한 정보자산을 임의로 외부에 누출해서는 아니 된다.

### 제5조(정보보호 조직체계)

회사는 정보보호 정책의 추진방향 및 계획에 대한 심의 및 의결을 위해 정보보호위원회(필요시 인사위원회로 대체할 수 있다.)를 구성하여 회사의 지속 가능성을 보장하고 정보보호사고 시 시스템 및 자원의 피해를 최소화 한다.

# 제 3 장 관리의무

#### 제6조(인적 보안)

- 1. 회사의 모든 임직원은 정보보호관련규정을 준수하여 업무를 수행하여야 한다
- 2. 임직원은 거래 당사자에게 회사의 정보보호관련규정을 사전에 인지할 수 있도록 설명할 의무가 있다.
- 3. 임직원이 정보보호관련규정을 위반하여 회사에 유/무형의 손실을 입히거나 이미지를 훼손한 경우에는 인사위원회에 회부하여 징계할 수 있으며, 필요시 관계기관과 협조하여 원인을 규명하고, 관련 법에 따라 사법당국에 고발조치 또는 회사의 피해에 대하여 민,형사상의 모든 책임을 물을 수 있다.

4. 회사의 임직원은 정보보호에 대한 책임과 역할을 분명히 하고 내부인에 의한 정보보호 사고를 예방하기 위한 목적으로 시행되는 정보보호 서약서의 내용을 숙지 후 서명, 날인해야 한다.

### 제7조(보안 점검 및 감사)

회사는 정보보안 사고를 예방하고, 보안관리가 제대로 수행되고 있는지 검출, 개선함으로써 경영 목표 달성을 지원할 수 있도록 정보보호 관리체계의 점검에 대한 제반사항을 규정하고 점검 활동을 이행하며 점검 후 취약 사항에 대한 조치를 수행한다.

#### 제8조(정보보호 교육)

정보보호 담당부서는 전 임직원을 대상으로 정보보호 인식제고 및 운영에 필요한 교육계획을 수립하여 정기적으로 시행하여야 한다.

#### 제9조(정보 자산의 활용 및 관리)

- 1. 회사는 중요 정보 자산을 분류하고 훼손, 변조, 도난, 유출 등의 다양한 형태의 침해 위 협으로부터 초래되는 위험을 제거하거나 최소화 하기 위한 규정을 정하여 정보자산을 관 리하여야 한다.
- 2. 모든 임직원 및 외부인은 직무상 부여된 정보 자산에 접근하여 정보자산을 활용할 권한 이 부여됨과 동시에 해당 정보를 보호하여야 할 책임을 지며 부주의, 부적절한 행위, 혹은 고의나 과실로 정보자산을 허용되지 않는 자에게 노출시켜서는 안 된다.
- 3. 분류된 정보 자산은 소유권자 또는 해당 부서의 장 승인 없이 외부에 공개, 유출해서는 안 된다.

#### 제10조(물리적 보안)

- 1. 회사는 특별한 보호가 필요한 시설 및 장비를 권한 없는 자의 물리적 접근 및 각종 재난 으로부터 보호하기 위하여 보호구역을 정의하고 이에 따른 보안 대책을 수립, 이행하여야 한다.
- 2. 물리적 보안을 담당하는 조직은 물리적 보안관리를 위한 세부사항을 정의하고 이에 따라 필요한 조치를 이행하며 주기적으로 검토하여야 한다.

## 제11조(개인정보보호)

- 1. 회사는 신용정보의 이용 및 보호에 관한 법률 등 관련 법령 기준에 부합하도록 개인정보 보호 정책 및 관리 기준을 수립하고 이를 시행하여야 한다.
- 2. 또한 임직원 개인정보와 업무상 취급하는 개인정보를 체계적으로 관리하여 도난, 유출, 훼손으로 부터 보호하고 오남용 되지 않도록 임직원 개인정보와 개인정보보호 담당 조직을 지정하여야 한다.

## 제12조(관련법령)

- 1. 개인정보보호법
- 2. 신용정보의 이용 및 보호에 관한 법률
- 3. 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 4. 부정경쟁방지 및 영업비밀보호에 관한 법률
- 5. 정보보호산업의 진흥에 관한 법률

## 부 칙

1. 본 규정은 서기 2022년 09월 30일 부터 시행한다.