개인정보 보호 행동지침

본 지침은 개인정보를 취급하는 회사 임직원 및 외부 협력업체의 임직원, 프리랜서에 적용한다.

*** 컴퓨터 사용 보안**

1. 컴퓨터를 사용하지 않는 경우, 로그오프를 한다.
 - 로그인 패스워드 설정
 - 시스템을 사용하지 않을 때나, 자리를 일정기간 비울 경우엔, 반드시 로그아웃을 하여 비인가자들의 접근을 방지한다. 또한 화면보호기는 항상 "10분 이내"로 설정한다.
2. 주요 파일은 반드시 암호화하며, 공유폴더에는 기밀자료를 보관하지 않는다.
 - 사내 주요 정보 등급(일반, 대외비, 비밀)에 따라 업무용 PC내의 기밀 파일은 반드시 암호화 하여 저장한다.
 - 공유폴더에 기밀자료를 보관하지 아니하며, 반드시 비밀번호를 설정하도록 한다.
3. 프로젝트 수행 중 취득한 고객에 대한 정보 및 산출물 등을 개인 PC 또는 사내 서버등을 통해 보관하거나, USB 등으로 반출 하여서는 안 된다.
4. 악성코드가 의심되는 이메일은 실행하지 않고, 삭제한다.
5. 협력업체나 외부직원이 프로젝트 수행 시에도 "반드시 보안서약서를 작성하고, ㈜핑거 개인정보보호 내부관리규정을 준수 한다.

*** 사무실 보안**

1. 책상 위에 문서나 저장매체를 방치하지 않는다.
2. 공용 캐비닛에는 책임자를 지정하고 퇴실할 경우에는 시건 후 열쇠를 안전한 곳에 보관한다.
3. 중요 정보가 담긴 저장매체, 출력된 문서 또는 PC 등은 비인가자의 접근으로부터 보호한다.
4. 당장 필요하지 않은 중요정보가 담긴 인쇄물, 저장매체, 휴대용 전산장비는 시건 장치가 설치된 캐비닛 또는 서랍장에 보관하고, 중요문서는 반드시 문서 세절기를 통해 파쇄한다.
5. 내부 대외비 문서 (규정, 지침, 내부 직원 정보, 사업계획, 영업비밀 기타 등) 출력자료, Data등이 외부에 유출되거나 외부손님 방문 시 문건이 Open되지 않도록 각별히 주의한다.
 (외부인에게 메일발송, P2P등 파일업로드, 기타 등등)
6. 외부 업체 명함 및 기타 프리랜서등의 명함은 책상 위에 방치하지 않고, 시건 장치가 설치된 캐비닛이나 서랍장에 보관한다.
7. 퇴근 시 정리 정돈 한다.
 - 개인 PC 종료 및 책상정리 후 퇴근한다.
 - 문서등은 반드시 캐비닛 또는 서랍장에 넣고 퇴근한다.

*** 패스워드 보안 준수**

1. 시스템에서 초기 패스워드를 할당하는 경우, 사용자는 해당 패스워드를 새로운 패스워드로 변경하여 사용한다.
2. 패스워드 변경 시, 변경될 패스워드는 이전 패스워드와 연관성이 없어야 한다.
3. 자신의 패스워드가 제 3자에게 노출되지 않도록 해야 한다.
 - 패스워드를 메모지에 기록할 경우 안전한 장소에 보관하도록 함

4. 제3자에게 자신의 패스워드와 관련된 정보 및 힌트를 제공하지 않아야 한다.
5. 자신의 패스워드가 제3자에게 노출되었을 경우, 즉시 새로운 패스워드로 변경해야 한다.

*** 패스워드 가이드**

1. 영어 대문자, 영어 소문자, 숫자 중 2종류 이상의 문자를 사용할 것
2. 최소 길이는 8자리
3. 최대 3개월 마다 교체해야 함
4. 동일한 비밀번호 사용 제한 : 2개의 비밀번호를 교대로 사용하지 않는다.
5. 생성한 비밀번호에 12345678 등과 같은 일련번호, 전화번호 등과 같은 쉬운 문자열이 포함되지 않도록 한다.
6. love, happy 등과 같은 잘 알려진 단어 또는 키보드 상에서 나란히 있는 문자열도 포함되지 않도록 한다.

*** 지적재산권 보안**

1. 회사 내에서 사용하는 모든 PC에는 정식으로 등록된 소프트웨어 (회사가 라이센스 계약을 체결, 구매한 소프트웨어) 를 사용하여야 하며, 불법 소프트웨어의 사용을 금한다. [저작권법에 의거]
2. 협력업체나 외부직원의 경우 소속 회사 보유 정품 소프트웨어 또는 개인의 정품 소프트웨어를 사용한다.

* 다음의 경우 불법 소프트웨어 사용에 해당한다.
- 상용 소프트웨어 인증(License) 받지 아니한 자가 사용하는 경우
- 쉐어웨어(Shareware)를 회사 내에서 사용하는 경우
- 번들 소프트웨어 (Bundle) 소프트웨어를 무단으로 배포하여 사용하는 경우
- 기관 및 기업에 공개되지 않은 프리웨어를 사용하는 경우
- 사외 정식 소프트웨어 (가정용 등) 사내에서 무단으로 사용하는 경우
- 쉐어웨어를 크랙 (Crack) 하여 정품처럼 사용하는 경우 (제품등록번호 무단복제 포함)
- 기타 정보보안 주관부서에서 승인을 받지 않은 소프트웨어를 사용하는 경우

*** 테스트 정보 보안**

1. 회사 금융관련 서비스를 이용 및 운용하기 위한 테스트 보안 정보를 이용함에 있어 금융 카드사의 보안 규정, 지침, 정책 등을 준수한다.
2. 직무상 알게 된 비밀, 재산, 신용, 기타 보안사항에 대해서는 외부에 누설하지 않는다.
3. 업무종료 후에도 업무 중 지득한 사실, 업무, 거래, 고객, 거래선 등 일체의 사항에 관한 정보를 누구에게도 공개하거나 누설하지 않는다.
4. 테스트 계좌 정보를 사사로이 유용하거나 은행업무를 빙자하여 사리를 꾀하는 일이 없도록 한다.
5. 관련 업무를 진행 하게 될 경우 반드시 해당 서약서를 작성한다.