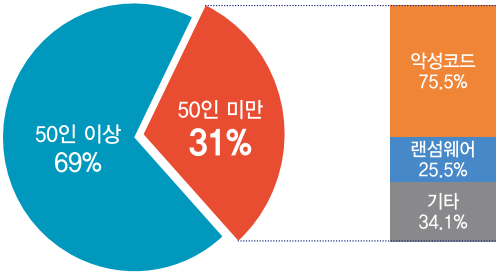
창업기업을 위한
정보보호 가이드라인

Security Guide for Start-up

과학기술정보통신부
KISA 한국인터넷진흥원

기업 보안 현황

'2017년 정보보호 실태조사' 에서 침해사고 피해 경험이 있다고 답한 기업 중 50인 미만의 기업이 전체의 약 31%



창업기업 및 중소기업의 정보보호 미흡으로 인한 피해 사례

– 최근 3년간 중소기업 기술유출 피해액 '3,021억'
– A업체 : 이메일 해킹되어, 8만달러 해커에게 송금 ('18.8)
– B업체 : 개인정보 유출로 과징금 3억원 행정처분 ('17.9)

창업 단계 고려 사항

정보보안 체크리스트

START

창업준비를 위한 아이템을 구상하였는가?

YES

NO → 2.1.1 창업아이템 및 지식재산권 이해하기

아이템에 필요한 특허 및 지식재산권 확보를 하였는가?

NO → 2.1.2 특허 및 지식재산권 보호 방법 알아보기

YES

회사 설립을 위한 사업자 등록 및 업종별 확인사항을 파악 하였는가?

NO → 2.2.1 사업자 등록 및 업종별 필요사항

YES

회사에 필요한 정책 및 규정을 만들었는가?

NO → 2.2.2 정책 수립 및 관리적 보호조치

YES

홈페이지 또는 모바일 APP 개발에 필요한 보호조치를 적용하였는가?

NO → 2.3.1 홈페이지 구축 시 보호조치 사항

NO → 2.3.2 모바일 APP 구축 시 보호조치 사항

YES

개인정보 처리업무를 외부 업체에 위탁 시 관리 · 감독 하고 있는가?

NO → 2.3.3 외부 수탁업체 관리하기

YES

홈페이지를 통해 수집한 고객의 개인정보의 유효 기간제를 인지하고 있는가?

NO → 2.4.1 개인정보 유효기간제 이해하기

고객정보를 이용하여 광고성 정보 전달 시 필요한 조치를 하고 있는가?

NO → 2.4.2 광고성 정보 전송 시 유의사항

YES

해외 시장에 서비스 제공 시 국가별 요구사항을 검토하였는가?

NO → 2.4.4 글로벌 시장 진출 시 국가별 법률 검토

법률에서 요구하는 기술적 · 물리적인 보호조치를 적용하였는가?

NO →

- 2.4.3-(1) 홈페이지 취약점 진단
- 2.4.3-(2) 접속기록 및 접근권한 검토
- 2.4.3-(3) 업무 시 행동 수칙
- 2.4.3-(4) 개인정보 유출 통지신고
- 2.4.3-(5) 망법대상자 이용내역통지 · 망분리 · SNS

YES

창업기업에게 필요한 정보보호 준수 사항 완료!

창업 예비단계

지식재산권이란?

지식재산이란 돈이 되는 지식, 정보, 기술, 표현, 표시로써 타인이 쉽게 모방 할 수 있는 무형재산이기 때문에 법률에 따라 절차와 요건을 충족하여 보호받을 수 있다

지식재산권 보호방법

자신의 영업비밀이라는 것을 입증해 줄 수 있는 증명서비스를 이용하는 방법이 있다.

- **영업비밀 원본증명서비스** | www.tradesecret.or.kr
  한국특허정보원의 영업비밀보호센터에서 운영
- **기술자료 임치센터** | www.kescrow.or.kr
  대 · 중소기업협력재단에서 운영

회사 설립 및 신고단계

신고/등록/허가 필요 업종

구분	업종	유관법률
신고	부가통신사업	전기통신사업법
신고	통신판매업	전자상거래 등에서의 소비자보호에 관한 법률
신고	소프트웨어사업자	소프트웨어산업 진흥법
등록	인터넷발송 문자사업자	전기통신사업법
등록	게임제작업/배급업	게임산업진흥에 관한 법
허가	위치정보사업자	위치정보의 보호 및 이용 등에 관한 법률

책임자 지정 및 정책 수립

- 법률 상 지정 요건 및 업무, 자격요건 등을 확인하고 개인정보보호 책임자 및 정보보호 최고책임자 지정(사업주, 대표자, 임원 등으로 구성)
- 내부 관리 계획 마련
  예시 〉 www.privacy.go.kr/(개인정보보호 종합포털) 〉 자료마당 〉 참고자료 〉 제목:개인정보 내부 관리계획

개업 준비단계

홈페이지 구축 시 유의사항

운영할 시스템에 맞는 법령('개인정보보호법', '정보통신망법')을 검토하고 위반사항이 없도록 한다

① 기획

① 개인정보 수집 최소화 방안 마련 : 필요한 정보만 수집
② 동의 획득 시 유의사항 : 중요내용 강조, 동의 여부 선택
③ 개인정보 파기 방안 : 목적달성 및 이용기간종료 시 파기
④ 주민등록번호 대체수단 적용 검토 : 휴대폰, 아이핀, 공인인증서
⑤ 개인정보 처리시 적용할 암호화 방식 결정 :
일방향 암호화 및 안전한 암호 알고리즘 사용
⑥ 비밀번호 정책 수립 및 반영 : 영문자 + 숫자 + 특수문자 8자 이상
⑦ 개인정보 처리방침 작성 : 법률 요구사항 반영 및 공개

② 개발 · 구축

① '홈페이지 SW 개발보안 가이드'를 고려한 홈페이지 개발
② 보안대책 마련(참고 : www.kisa.or.kr/public/laws/laws2.jsp)
홈페이지 구축 시 유의사항

외부 수탁업체 관리

홈페이지 구축 및 운영, 고객정보를 이용한 홍보 텔레마케팅, 상품배송을 위한 택배사 등 개인정보 업무를 외부 업체에 위탁할 경우 발생할 수 있는 보안 위협에 대해서도 보안 강화를 위한 방안을 마련해야 한다.

침해사고 예방법

정품 프로그램 사용하기

공유폴더 사용 최소화하고 사용시 비밀번호 설정

공인인증서는 별도의 저장매체에 보관

의심스러운 메시지는 바로 삭제하기

백신프로그램 설치하고 바이러스 검사하기

비밀번호 설정하고 주기적으로 변경하기

신뢰할 수 없는 웹사이트 방문하지 않기

최신 버전의 운영체제 SW 사용하기

공식마켓에서 앱다운로드 하기

모르는 사람이 보낸 이메일, 파일은 열어보지 않기

기술안내서 가이드

정보보호 및 개인정보보호 관련 (IT 시스템, 정보시스템 개발, 운영 및 일반 업무)를 위한 기술안내서를 제공하고 있습니다.

– **한국인터넷진흥원** | www.kisa.or.kr
자료실 〉 기술안내서 가이드

사업 운영단계

고객관리

개인정보 유효기간제 : 1년 동안 서비스를 이용하지 않는 고객의 개인정보는 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장 · 관리해야 한다.

광고성 정보 전송

① 광고성 정보 전송 시 유의사항

- 사전 수신동의 (Opt-in)를 받아야 함
- 수신거부 및 수신동의 철회 시 광고전송 금지
- 야간광고(오후 9시 ~ 다음날 오전 8시)시 별도 사전 동의 필요

② 전자우편, 팩스 등을 통한 정보 전송 시 표기의무 사항

- 광고성 정보가 시작되는 부분에 (광고) 표시
- 전송자의 명칭, 전화번호 또는 주소를 표시
- 수신에 대한 철회 방식 안내

기술적 관리적 물리적 보호조치

① 취약점 진단 수행

- 운영하고 있는 시스템은 연 1회 이상 취약점 점검 실시

② 접속기록 및 접근권한 주기적 검토

- 접속기록은 반기별 1회 이상(정보통신서비스 경우 월 1회) 정기적으로 확인 및 감독

③ 업무 시 보안 행동 수칙

- 저장매체 무단 반출 금지, 클린데스크 실천, 비밀문서 파쇄, 통제구역 출입제한, PC 및 문서 암호설정

④ 개인정보 유출 통지 · 신고

- 유출사실 인지 후 지체없이 정보주체(이용자)에게 알리고, 기관에 신고(한국인터넷진흥원 118)

글로벌 시장 진출

사업소재지 또는 서비스 제공 대상이 해외에 있을 경우 해당 관련법을 검토하여 적용하여야 한다.(특히 2018년 유럽 일반 개인정보보호법은 모든 EU 회원국에 대한 강행규정으로 위반 시 과징금 등 행정처분이 부과될 수 있음)

알아두면 유용한 사이트

KISA 보호나라 | www.boho.or.kr
해킹 · 바이러스, 개인정보 침해, 불법스팸신고에 대한 정보를 제공

온라인 개인정보보호 포털 | www.i-privacy.kr
정보통신망법 개정안내, 위치정보보호 교육, 주민등록번호 대체수단, 업종별 개인정보보호 교육 무료 제공

개인정보보호 종합지원 포털 | www.privacy.go.kr
개인정보보호법 관련 법 · 제도 · 교육정보를 제공

정보보호산업진흥포털 | www.kisis.or.kr
정보보호산업에 대한 종합적인 지원 및 핀테크 기술지원 등을 제공

과학기술정보통신부
KISA 한국인터넷진흥원