

『개인정보 유출 대응 매뉴얼』 요약

< 개인정보 유출 대응 절차(요약) >

1 개인정보 유출 신속 대응팀 구성



2 유출 원인 파악 및 추가 유출 방지조치

신속 대응팀

- ◆ 개인정보 침해사고 접수 및 사실 여부 확인
- ◆ 개인정보 유출 사고 원인 파악
- ◆ 접근통제, 모니터링 강화
- ◆ 유출된 개인정보 회수

3 개인정보 유출 신고 및 통지

신속 대응팀



4 이용자 피해구제 및 재발방지 대책 마련

신속 대응팀



① 개인정보 유출 신속 대응팀 구성·운영

◇ 개인정보 유출 사실을 알게 된 경우, 개인정보보호책임자는 즉시 CEO에게 보고하고 「개인정보 유출 신속대응팀」을 구성하여, 추가 유출 및 이용자 피해 발생 방지를 위한 조치를 강구

○ 개인정보보호 책임자*는 개인정보 유출사실을 알게 된 경우 신속히 CEO에게 보고

* 개인정보 유출사실을 발견한 임직원은 즉시 개인정보보호 책임자에게 신고

○ 「개인정보 유출 신속대응팀」을 구성하여 추가 유출 및 이용자 피해발생 방지를 위한 조치를 강구

② 유출원인 파악 및 추가유출 방지조치

◇ 개인정보 유출원인을 신속히 파악한 후 유출경로별 추가유출 방지를 위한 개선조치 실시

○ (해킹) 추가유출 방지를 위해 시스템 일시정지, 비밀번호 변경 등 긴급조치를 시행하고, 미비한 부분은 원인 파악 후 즉시 보완조치

※ 기술력 등 한계로 자체 긴급조치가 어려운 경우 한국인터넷진흥원에 기술 지원 요청

○ (내부자 유출) 개인정보 유출자의 접속이력 등을 확인하여 비정상적인 접속인 경우 우회경로를 확인 후 접속 차단

※ 반드시 접속계정, 접속권한 등을 검토하여 추가적인 유출여부를 확인하여야 하며, 유출된 개인정보 회수를 위한 모든 조치를 강구

○ (이메일 오발송) 이메일 회수가 가능한 경우 즉시 회수 조치하고, 불가능한 경우 수신자에게 즉시 삭제 요청

※ 메일서버 외 첨부파일서버(대용량 메일 등)를 이용하는 경우 해당 서버 운영자에게 삭제 요청

○ (개인정보 노출) 검색엔진에 노출된 경우 원사이트의 개인정보 삭제, 검색엔진에 노출된 개인정보 삭제를 요청하고, 필요 시 로봇배제 규칙을 적용하여 검색엔진의 접근을 차단

3 개인정보 유출 신고 및 통지

◇ 개인정보 유출사실을 알게 된 경우 즉시 관계기관 신고 및 이용자 통지 이행

- (침해사고 신고) 경찰청(사이버안전국)에 범죄수사 요청과 함께 미래부·한국인터넷진흥원에 침해사고를 신고
 - ※ 해커 등 유출자 검거를 통한 개인정보 회수를 위한 모든 수단 강구
- (유출 신고) 방통위·한국인터넷진흥원에 즉시(24시간 이내) 확인된 사항을 중심으로 신고하고 이후 추가 신고 병행
 - ※ “개인정보보호 포털”(www.i-privacy.kr)을 통해 신속히 신고
- (유출 통지) 이용자에게 즉시(24시간 이내) 확인된 사항을 중심으로 개별 통지하고, 추가로 확인되는 내용은 개별 또는 홈페이지를 통해 신속히 통지 실시
 - ※ 통지를 할 때에는 이용자가 실제 확인 가능하도록 이용빈도가 높은 방법(예: 전화통화/문자/이메일/팩스 등)을 우선 활용하여 통지하는 것이 바람직
 - ※ 대규모 유출사고의 경우 24시간 이내 전체 통지가 기술적으로 불가능한 경우가 있어, 이 경우 우선적으로 홈페이지 팝업창 등을 통해 게시한 후 개별 통지 및 유출 확인절차를 병행토록 함
 - ※ 일부 정보만 유출된 이용자의 경우에도 통지 의무가 있음을 명시
- (유출 확인절차 마련) 이용자가 홈페이지 등을 통해 유출사실을 확인할 수 있도록 절차를 운영
 - ※ 이 과정에서 추가적인 유출이 발생하지 않도록 웹 취약점 제거, 전송구간 암호화(보안서버 등) 이행, 주민번호 사용 금지 등 유의점을 안내

4 이용자 피해구제 및 재발방지 대책 마련

◇ 이용자 피해구제 방법을 안내하고, 유사 사고의 재발방지를 위해 대책 마련

- (개인정보 유출사고 전파) 한국인터넷진흥원과 협의하여 “사업자 핫라인”을 통해 사고 사실을 전파

- (이용자 피해구제 관련 대응) 안내 스크립트와 통지문을 작성하여 이용자 문의에 신속하게 대응하고, 피해구제 절차*를 안내
 - * 개인정보 분쟁조정 신청, 법정·징벌적 손해배상 신청, “보이스피싱 지킴이 홈페이지”(금감원·경찰청) 안내 등
 - * 개인정보 유출로 인한 2차 피해 유형 및 이용자 대응 요령 안내 병행
- (유출 원인분석 및 재발방지 대책 마련) 유출사고 재발 방지를 위하여 취약점 분석·개선 및 개인정보보호 교육 실시