표준 개인정보 유출사고 대응 매뉴얼

2016. 12.

행정자치부  KISA 한국인터넷진흥원
본 매뉴얼은 「개인정보보호법」의 적용을 받는 개인정보처리자를 대상으로 합니다.

적용대상

업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통해 개인정보를 처리하는 공공 및 민간 부문의 모든 개인정보처리자

즉, 제조업, 서비스업 등 국내 380 만 전체 사업자 대상이며, 중앙행정기관·지자체는 물론 국회·법원·헌법재판소·중앙선거관리위원회 등 헌법기관과 협회·동창회 등 비영리단체도 대상이 됩니다.

본 매뉴얼은 「표준 개인정보 보호지침」(행정자치부 고시 제 2016-21호, 2016.6.30.) 제29조(개인정보 유출 사고 대응 매뉴얼 등)에 따라, 기관·기업이 유출 사고 발생 시 피해 발생을 최소화하기 위해 마련해야 하는 「개인정보 유출 사고 대응 매뉴얼」에 대한 최소한의 사항을 포함하여 제시한 것입니다.

관계법령

표준 개인정보 보호지침

제29조(개인정보 유출 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출 사고 대응 매뉴얼」을 마련하여야 한다.
1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1항에 따른 개인정보를 처리하는 개인정보처리자
② 제1항에 따른 개인정보 유출 사고 대응 매뉴얼에는 유출 통지·조회 절차, 영업장·인터넷화선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등의 포함하여야 한다.
③ 개인정보처리자는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

각 기관과 기업은 본 매뉴얼을 조직의 특성 및 환경에 맞게 보완하여 사용하시면 됩니다.
※ 파란색으로 표기된 부분은 조직에 맞게 수정하여 사용하십시오.
1. 개요 .................................................................
   1.1 목적 ................................................................
   1.2 법적 근거 ......................................................
   1.3 적용 범위 ......................................................
   1.4 단계별 프로세스 ..............................................
   1.5 유출대응 업무수행 체계 .................................

2. 개인정보 유출사고 대응 필수 절차 ..........................
   2.1 유출통지·조회 절차 ........................................
   2.2 유출통지 신고 절차 ........................................
   2.3 현장 혼잡 최소화 조치 ....................................
   2.4 고객 민원 대응 조치 ........................................
   2.5 고객 불안 해소조치 .........................................
   2.6 피해자 구제 조치 ............................................

□ [붙임 1] 유출통지 방법 ........................................
□ [붙임 2] 개인정보 유출 신고기관 연락처 ..................
□ [붙임 3] 사고대응 흐름도 .................................
1 개요

1.1 목적

‘개인정보 유출사고 대응 매뉴얼’은 ‘개인정보보호법’ 및 같은법 시행령, 시행규칙에 따라 개인정보 유출사고에 대한 신속하고 체계적인 대응을 목적으로 한다.
※ 관련근거: 표준 개인정보보호지침 제29조(개인정보 유출 사고 대응 매뉴얼 등)

1.2 법적 근거

개인정보보호법(법률 제13423호) 및 시행령, 시행규칙
표준 개인정보보호 지침(행정자치부고시 제2016-21호)
개인정보의 안전성 확보조치 기준(행정자치부고시 제2014-7호)

1.3 적용범위

해킹, 분실, 도난 등으로 인해 개인정보가 내·외부에 의하여 유출된 경우에 적용된다.
유출된 개인정보의 종류, 수량, 암호화 여부, 유출시기, 개인정보취급자에 의한 고의, 과실 여부 등을 묻지 아니한다.

가이드

○ 단 1건만 유출되어도 정보주체(예: 고객, 회원)에 대한 통지 등 의무를 이행하고, 1만명 이상 유출된 경우 행정자치부 및 한국인터넷진흥원에 신고
○ 유출된 정보(예: 비밀번호, 계좌번호 등)가 암호화되어 있어도 정보주체 통지 의무 이행
개인정보 유출의 개념

표준 개인정보보호지침 제 25 조 (개인정보의 유출) 개인정보의 유출은 법령이나 개인정보 처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달된 경우
### 단계별 프로세스

<table>
<thead>
<tr>
<th>단계</th>
<th>상세 업무</th>
<th>비고</th>
</tr>
</thead>
<tbody>
<tr>
<td>사고인지 및 긴급조치</td>
<td>○ 개인정보 유출사고 신고 접수 및 사고인지 &lt;br&gt; ○ 유출사고 대응센터 소집 및 유관기관 협조체계 확인 &lt;br&gt; ○ 피해 최소화를 위한 긴급조치 수행 &lt;br&gt; ※ 유출된 개인정보 삭제조치 및 기술지원 요청</td>
<td></td>
</tr>
<tr>
<td>↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>정보주체 유출통지</td>
<td>○ 정보주체에게 개인정보 유출사실 통지(5 일이내)</td>
<td>세부내용 2.1 참고</td>
</tr>
<tr>
<td>↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>개인정보 유출신고</td>
<td>○ 1 만명 이상의 개인정보 유출사 행정자치부 또는 한국인터넷 뷰티중요(privacy.go.kr)에 유출신고</td>
<td>세부내용 2.1 참고</td>
</tr>
<tr>
<td>↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>민원대응반 운영</td>
<td>○ 개인정보유출사고 규모 및 성격에 따라 민원대응반 구성</td>
<td>세부내용 2.2 참고</td>
</tr>
<tr>
<td>↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>고객민원 대응</td>
<td>○ 2 차피해자별로한고객민원대응및고객불안해소조치</td>
<td>세부내용 2.3~4 참고</td>
</tr>
<tr>
<td>↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>피해구제 절차</td>
<td>○ 개인정보 유출에 대한 피해구제 절차 안내</td>
<td>세부내용 2.5 참고</td>
</tr>
<tr>
<td>↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>보안기능 강화</td>
<td>○ 사고 원인 분석 및 보안 강화·기능 개선</td>
<td></td>
</tr>
<tr>
<td>↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>결과 보고</td>
<td>○ 기관장 및 이사회에 개인정보 유출사고 결과보고서 작성 및 보고</td>
<td></td>
</tr>
<tr>
<td>제발방지</td>
<td>○ 개인정보 유출사고 사례 전과 교육 및 개선 대책 시행</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.5 유출대응 업무수행 체계

조직체계(유출사고 대응센터)

<table>
<thead>
<tr>
<th>조직별</th>
<th>담당자</th>
<th>담당 업무</th>
</tr>
</thead>
<tbody>
<tr>
<td>개인정보보호 책임자</td>
<td>○○팀장</td>
<td>•유출사고 대응 총괄 지휘</td>
</tr>
<tr>
<td>총괄대응본부</td>
<td>○○팀장</td>
<td>•유출사고 인지, 접수, 전파</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•유출사고 대응 절차 수립</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•정보주체에게 유출사실 통지</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•행정자치부 또는 전문기관에 유출통지 사고 신고</td>
</tr>
<tr>
<td>분석반</td>
<td>○○팀장</td>
<td>•유출 사실 확인, 조사 및 원인 분석</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•사고내용 세부조사</td>
</tr>
<tr>
<td>복구반</td>
<td>○○팀장</td>
<td>•외부요인에 의한 유출의 경우, 유관 기관과 협조하여 사고 처리 지원</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•시스템 복구 및 백업(유지보수/협력업체 포함)</td>
</tr>
<tr>
<td>민원대응반</td>
<td>○○팀장</td>
<td>•고객 개별 통지문 안내에 따른 후속업무(민원 등) 진행</td>
</tr>
<tr>
<td>(온라인, 오프라인)</td>
<td></td>
<td>•고객상담센터, 소비자보호 방안 마련(필요시 유관부서와 협조)</td>
</tr>
<tr>
<td>조직별</td>
<td>담당자</td>
<td>담당 업무</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>홍보반</td>
<td>○○팀장</td>
<td>• 유출사고 관련 대외기관(언론사 등) 대응</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 유출사고 대고객 안내문 문구 최종 검토</td>
</tr>
<tr>
<td>법무반</td>
<td>○○팀장</td>
<td>• 법률상 대응방안, 의사결정 사항 등 정책적 판단사항 검토 및 결정</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 유출사고 관련 수사기관 경과사항 대응 및 대책반 공유</td>
</tr>
</tbody>
</table>
비상연락망
- 유출사고 대응센터

<table>
<thead>
<tr>
<th>조직별</th>
<th>담당자</th>
<th>전화번호</th>
<th>이메일</th>
</tr>
</thead>
<tbody>
<tr>
<td>개인정보보호책임자</td>
<td>성함, 직책 명시</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>총괄대응본부</td>
<td>○○팀장</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>분석반</td>
<td>○○팀장</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>복구반</td>
<td>○○팀장</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>민원대응반</td>
<td>○○팀장</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>홍보반</td>
<td>○○팀장</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>법무반</td>
<td>○○팀장</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
</tbody>
</table>

- 협력업체/유지보수업체

<table>
<thead>
<tr>
<th>업체명</th>
<th>담당 시스템</th>
<th>담당자</th>
<th>전화번호</th>
<th>이메일</th>
</tr>
</thead>
<tbody>
<tr>
<td>○ ○기업</td>
<td>○ ○시스템</td>
<td>성함, 직책 명시</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>○ ○기업</td>
<td>○ ○시스템</td>
<td>성함, 직책 명시</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>기업</td>
<td>시스템</td>
<td>성함, 직책 명시</td>
<td>연락처</td>
<td>이메일</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>----------------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>오오기업</td>
<td>오오시스템</td>
<td>성함, 직책 명시</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>오오기업</td>
<td>오오시스템</td>
<td>성함, 직책 명시</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
<tr>
<td>오오기업</td>
<td>오오시스템</td>
<td>성함, 직책 명시</td>
<td>02-000-0000 (010-000-0000)</td>
<td><a href="mailto:OOO@ooo.kr">OOO@ooo.kr</a></td>
</tr>
</tbody>
</table>
2 개인정보 유출 사고 대응 필수 절차

2.1 유출 통지·조회 절차

<table>
<thead>
<tr>
<th>가이드</th>
</tr>
</thead>
<tbody>
<tr>
<td>o 개인정보처리자는 개인정보보호법 제34조 1항에 따른 통지 절차를 마련하고 이에 대한 내용을 다음에 기술</td>
</tr>
<tr>
<td>o 개인정보처리자는 1만명 이상 정보주체의 개인정보 유출 사고 발생 시 당국에 대한 신고관련 절차를 마련하고 이에 대한 내용을 다음에 기술</td>
</tr>
<tr>
<td>o 개인정보처리자는 고객(정보주체)이 홈페이지 등을 통해 자신의 개인정보가 유출되었는지 확인할 수 있는 절차를 만들고 이에 대한 내용을 다음에 기술</td>
</tr>
<tr>
<td>o (개인정보 처리 업무 위탁 시) 1차적인 유출 신고 및 통지 의무는 위탁자에게 있으므로, 유출 사고 발생 시 수탁자와의 대응 절차를 마련하고 이에 대한 내용을 다음에 기술</td>
</tr>
</tbody>
</table>

총괄대응본부는 유출 인원 등을 확인하여 [붙임 1]의 양식을 유출통지 방법에 따라 이용하여 정보주체들에게 유출 통지

- 통지 항목 : ① 유출된 개인정보의 항목, ② 유출 시점과 그 경위, ③ 피해 최소화를 위한 정보주체의 조치방법, ④ 기관의 대응조치 및 피해구제 절차, ⑤ 피해 신고 접수 담당부서 및 연락처

수탁사업자가 수탁 업무를 처리하는 과정에서 개인정보가 유출된 경우 즉시 위탁자에게 보고하도록 위.수탁계약서에 명시하고, 수탁사업자로부터 보고 받은 시점에서 지체 없이 유출 통지

1 만명 이상 유출시에는 홈페이지에 필수 유출통지 5개 항목을 7일 이상 공지하고, 정보주체가 유출 여부를 확인할 수 있는 별도 페이지 (http://ooo.com/119) 제공

- 1 만명 이하 유출시에도 유출사실을 홈페이지에 공개하여 정보주체가 피해를 예방할 수 있도록 하는 것이 바람직함
- 아이핀, 헌드폰 인증 등을 통한 정보주체 본인 확인 후 개인정보 유출 결과 조회
2.2 유출통지 신고 절차

(1 만명 이상 유출시) 인지 시점으로부터 5 일 이내 행정자치부 또는 한국인터넷진흥원에 유출 신고
※ 신고방법 : privacy.go.kr 접속 – 사업자 – 개인정보 민원 – 개인정보 유출신고
- 이후 OOO 홈페이지(개인정보처리자의 인터넷 홈페이지)에 필수 유출통지 5 개 항목을 7 일 이상 게재

(신고해야 할 내용) 정보주체에 대한 유출 통지 결과 및 피해 최소화를 위한 조치 결과

2.3 현장 혼잡 최소화 조치

가이드

- 물리적으로 개인정보가 소실되거나 운영 중인 개인정보가 침해당했을 경우, 해당 현장 혼잡 최소화를 위한 절차를 마련하고 이에 대한 내용을 다음에 기술

총괄대응본부는 O층 OO회의실 오프라인 창구를 개설
- 전화, 메일, 홈페이지, SNS 등 한 가지 이상의 채널을 선택하여 단일화된 민원대응 창구를 구축

<table>
<thead>
<tr>
<th>구분</th>
<th>채널</th>
<th>상세 내용</th>
</tr>
</thead>
<tbody>
<tr>
<td>오프라인</td>
<td>3층 OO 회의실</td>
<td></td>
</tr>
<tr>
<td>온라인</td>
<td>전화</td>
<td>02-000-0000</td>
</tr>
<tr>
<td></td>
<td>메일</td>
<td><a href="mailto:privacy@ooo.ooo">privacy@ooo.ooo</a></td>
</tr>
<tr>
<td></td>
<td>홈페이지</td>
<td><a href="https://ooo.ooo">https://ooo.ooo</a></td>
</tr>
<tr>
<td></td>
<td>SNS</td>
<td>#OOOO</td>
</tr>
</tbody>
</table>

복구반은 유출된 시스템의 이용을 제한하고 별도의 임시 시스템 구축을 통하여 기관의 업무 혼잡 방지
분석반은 대외 수사기관에 협조 할 수 있는 전담 인력 구성 및 대응
2.4 고객 민원 대응 조치

<table>
<thead>
<tr>
<th>가이드</th>
</tr>
</thead>
<tbody>
<tr>
<td>o 개인정보처리자는 고객(정보주체) 민원을 처리할 수 있는 체계를 만들고 이에 대한 내용을 다음에 기술</td>
</tr>
</tbody>
</table>

민원대응반은 유관부서(총괄대응본부, 법무반)과 협의하여 피해자 구제 방안, 수사 진행상황 등에 대한 외부 질의 답변 방향 결정

협의 방안을 토대로 민원대응 매뉴얼 작성 및 배포

민원대응 전담 인력: 회선 확인 및 대응 매뉴얼 교육

대외 적 접촉창구는 민원대응반으로 단일화하여 사내 및 대민 OOO 홈페이지(https://ooo.com)에 공지하고 타 팀에서 외부로부터 개인정보 유출관련 질문을 받으면 최대한 민원대응반으로 연결

기본적으로 민원대응반을 통해서 1차 민원 대응을 하고, 다음과 같은 경우 해당 부서에서 응대

<table>
<thead>
<tr>
<th>문의별</th>
<th>담당부서</th>
</tr>
</thead>
<tbody>
<tr>
<td>유출 확인 문의 대응</td>
<td>OO 팀 or OO 반</td>
</tr>
<tr>
<td>피해구제 관련 문의 대응</td>
<td>OO 팀 or OO 반</td>
</tr>
<tr>
<td>기타(000)</td>
<td>OO 팀 or OO 반</td>
</tr>
</tbody>
</table>

유출 규모와 상황을 고려하여 원활한 민원 처리를 위해 OO 통신사와 통신회선 증설 및 인터넷화선 확충과 관련된 계약수립

2.5 고객 불안 해소 조치

<table>
<thead>
<tr>
<th>가이드</th>
</tr>
</thead>
<tbody>
<tr>
<td>o 개인정보처리자는 고객(정보주체)이 유출된 개인정보로 인한 불안을 해소할 수 있는 체계를 마련하고 이에 대한 내용을 다음에 기술</td>
</tr>
</tbody>
</table>

OOO 홈페이지(https://ooo.com)에 유출 피해 최소화를 위해 현재 기관에서 실시하고 있는 노력에 대한 사항 공지(1 일 1 회 업데이트)
비밀번호, 신용카드번호 등 유출 시 비밀번호 변경, 카드 재발급 등을 할 수 있도록 유출 통지 시 함께 안내
※ 보이스피싱, 문자피싱 등 금융사기 예방을 위한 차단신청 기능(www.anti-phishing.or.kr) 등을 구체적으로 안내

[개인정보 유출 항목별 2차 피해 예방을 위한 안내사항]

<table>
<thead>
<tr>
<th>구분</th>
<th>세부 안내 사항</th>
</tr>
</thead>
<tbody>
<tr>
<td>아이디, 비밀번호 유출</td>
<td>비밀번호 변경 안내</td>
</tr>
<tr>
<td>카드번호 유출</td>
<td>카드 재발급 절차 안내</td>
</tr>
<tr>
<td>다량의 개인정보 유출</td>
<td>보이스피싱 등 2차 피해 예방 안내</td>
</tr>
</tbody>
</table>

2.6 피해자 구제 조치

가이드

○ 개인정보처리자는 고객(정보주체)의 피해를 구제할 수 있는 절차를 마련하고, 이에 대한 내용을 다음에 기술

시스템 오류 등 서비스 장애로 인한 고객의 민원 발생 시 유관부서와 협의하여 해결

(정보주체 요청이 있을 시) 회원 탈퇴 방법 안내 및 정보주체의 개인정보 삭제 조치
## 유출통지 방법

<table>
<thead>
<tr>
<th>구분</th>
<th>내용</th>
</tr>
</thead>
<tbody>
<tr>
<td>통지대상</td>
<td>정보주체</td>
</tr>
<tr>
<td>통지방법</td>
<td>◯ 서면, 이메일, FAX 전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법</td>
</tr>
<tr>
<td></td>
<td>◯ 위의 통지방법과 동시에 홈페이지에 공개하는 것이 바람직 - 단, 통지 및 조치 후에도 1만명 이상의 개인정보가 유출된 경우에는 서면 등</td>
</tr>
<tr>
<td></td>
<td>◯ 위의 통지방법과 함께 인터넷 홈페이지에 7일 이상 통지내용을 게재</td>
</tr>
<tr>
<td>통지내용</td>
<td>◯ 유출된 개인정보의 항목</td>
</tr>
<tr>
<td></td>
<td>◯ 유출된 시점과 그 경위</td>
</tr>
<tr>
<td></td>
<td>◯ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보</td>
</tr>
<tr>
<td></td>
<td>◯ 개인정보처리자의 대응조치 및 피해 구제절차</td>
</tr>
<tr>
<td></td>
<td>◯ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처</td>
</tr>
<tr>
<td>통지시기</td>
<td>유출사실을 발견할 때로부터 5일 이내</td>
</tr>
<tr>
<td>통지연기</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>○개인정보 유출확산방지를 위한 조치가 필요한 경우 연기 가능</td>
<td></td>
</tr>
<tr>
<td>- 개인정보가 유출되었을 것으로 의심되는 개인정보처리시스템의 접속 권한 삭제·변경 또는 폐쇄 조치</td>
<td></td>
</tr>
<tr>
<td>- 네트워크, 방화벽 등 내외시스템 보안점검 및 취약점 보완 조치</td>
<td></td>
</tr>
<tr>
<td>- 향후 수사에 필요한 외부의 접속기록 등 보존 조치</td>
<td></td>
</tr>
<tr>
<td>- 정보주체에게 유출 관련 사실을 통지하기 위한 유출확인 웹페이지 제작 등의 통지방법 마련 조치</td>
<td></td>
</tr>
<tr>
<td>- 기타 개인정보의 유출확산 방지를 위한 필요한 기술적·관리적 조치</td>
<td></td>
</tr>
<tr>
<td>○개인정보처리자는 위 각 항목의 조치를 취한 이후, 정보주체에게 다음 각 항목의 사실만 일차적으로 알리고 추후 확인되는 즉시 알릴 수 있음</td>
<td></td>
</tr>
<tr>
<td>- 정보주체에게 유출이 발생한 사실</td>
<td></td>
</tr>
<tr>
<td>- 통지내용 중 확인된 사항</td>
<td></td>
</tr>
</tbody>
</table>
개인정보 유출 표준 통지문안 (예시)

※ 유출된 항목, 유출된 시점과 경위가 확인되지 않아 통지문에 포함하지 않은 경우 추후 확인 되면 반드시 추가 통지
<table>
<thead>
<tr>
<th>표준 통지문안 예시</th>
<th>부가 설명</th>
</tr>
</thead>
</table>
| 귀하의 개인정보는 ○○○시스템에 저장·보관하다가 ○○○년 ○○월경 해커에 의한 해킹으로 유출되었습니다. | <유출된 시점과 경위>  
- 유출된 시점과 경위를 상세하게 설명 |
| 유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 주민등록번호, 이메일, 연락처 총 6 개입니다. | <유출된 항목>  
- 유출된 항목을 누락 없이 모두 나열 |
| 유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서비에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다. | <개인정보처리자의 대응조치>  
- 예시된 항목 외에도 조치한 내용 설명 |
| 혹시 모를 피해를 최소화하기 위하여 귀하의 비밀번호를 변경하여 주시기 바랍니다. | <피해 최소화를 위한 정보 주체의 조치방법>  
- 유출 경위에 따라 정보주체가 할 수 있는 방법을 안내  
- 예방 가능한 방법을 모두 안내 (보이스 피싱, 피싱 메일, 불법 TM, 스팰문자 등) |
| 아울러, 피해가 발생하였거나 예상되는 경우에는 아래 담당부서에 신고하시면 상실하게 안내와 상담을 해 드리겠습니다. | <개인정보처리자의 피해 구제절차>  
- 보상이나 배상이 결정된 경우에는 그 내용을 상세히 기재  
- 감독기관 등을 통한 구제 절차도 안내 |

- 피해 등 접수 담당부서: 0000 과  
- 피해 등 접수 전화번호: 02-2345-6789  
- 피해 등 접수 e-메일주소: abcd@efgh.co.kr  
- 피해 등 신고 접수 담당부서 및 연락처:  
  - 전담처리부서 및 대행을 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한
경우 해당 부서를 안내
## 둘임 2  개인정보 유출 신고기관 연락처

### □ 개인정보 유출 신고

<table>
<thead>
<tr>
<th>기 관 명</th>
<th>전화번호</th>
<th>인터넷사이트</th>
</tr>
</thead>
<tbody>
<tr>
<td>행정자치부</td>
<td></td>
<td><a href="https://www.privacy.go.kr/">https://www.privacy.go.kr/</a> (개인정보보호 종합지원포털)</td>
</tr>
<tr>
<td>한국인터넷 진흥원</td>
<td>118</td>
<td><a href="https://www.i-privacy.kr">https://www.i-privacy.kr</a> (개인정보보호포털)</td>
</tr>
<tr>
<td></td>
<td>(Fax:02-405-5229)</td>
<td><a href="http://www.kcc.go.kr">http://www.kcc.go.kr</a> (방송통신위원회)</td>
</tr>
<tr>
<td>방송통신 위원회</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### □ 관련기관 연락처

<table>
<thead>
<tr>
<th>기 관 명</th>
<th>전화번호</th>
<th>인터넷사이트</th>
</tr>
</thead>
<tbody>
<tr>
<td>대검찰청 사이버범죄 수사단</td>
<td>1301</td>
<td><a href="http://www.spo.go.kr/minwon">http://www.spo.go.kr/minwon</a></td>
</tr>
<tr>
<td>경찰청 사이버안전국</td>
<td>182</td>
<td><a href="http://cyberbureau.police.go.kr">http://cyberbureau.police.go.kr</a></td>
</tr>
</tbody>
</table>
붙임 3 사고대응 흐름도