GYEONGSANG
NATIONAL UNIVERSITY

대한민국을 대표하는 경남의 국가거점국립대학

경상국립대학교
Gyeongsang National University

# 개인정보 유출사고 대응 매뉴얼

2022. 7.

사 무 국
총 무 과

# < 목 차 >

# 1 개요

## 1.1 수립 목적

❍ ‘개인정보 유출사고 대응 매뉴얼’은 ‘개인정보 보호법’ 및 같은법 시행령, 시행규칙에 따라 개인정보 유출사고에 대한 신속하고 체계적인 대응을 목적으로 한다.

## 1.2 법적 근거

❍ 개인정보 보호법 제29조(안전조치의무), 제34조(개인정보유출 통지 등)

❍ 표준 개인정보보호 지침 제29조(개인정보 유출 사고 대응 매뉴얼 등)

❍ 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행)

## 1.3 적용범위

❍ 해킹, 분실, 도난 등으로 인해 개인정보가 내·외부자에 의하여 유출된 경우에 적용된다.

# 2 개인정보 유출 대응체계 구축

## 2.1 유출대응 업무수행 체계

❍ 조직체계(개인정보 유출 신속대응팀)

| | | |
|---|---|---|
| **개인정보 유출 신속대응팀** | **개인정보 보호책임자 (사무국장)** | · 개인정보 유출 대응 총괄 지휘 |
| | **개인정보 보호담당자** | · 유관기관에 개인정보 유출 신고<br>· 이용자에게 개인정보 유출 통지 |
| | **정보보안 담당자** | · 유관기관에 침해사고 신고<br>· 사고경위 분석, 시스템 복구 등 침해대응 |
| | **민원 대응반** | · 정부, 언론사, 이용자 민원 대응<br>· 이용자 피해구제 및 분쟁조정 기구 안내 |
| **전직원** | · 개인정보 유출 확인 시 부서장 또는 개인정보보호 부서에 신고<br>· 침해사고 발생 확인 시 부서장 또는 정보보호 부서에 신고<br>· 개인정보 유출 신속대응팀 요청에 따른 유출대응 지원 | |

## 2.2 비상연락망

### ❍ 유출 신속대응팀

| 조직별 | 담당자 | 전화번호 | 이메일 |
|---|---|---|---|
| 개인정보보호 책임자 | 사무국장 | 055-772-0065 | yhggh@gnu.ac.kr |
| 개인정보 보호담당자 | 총무과 개인정보 담당자 | 055-772-3141 | leeod@gnu.ac.kr |
| 정보보안 담당자 | 정보전산처 담당자 | 055-772-0613 | hancy@gnu.ac.kr |
| 민원대응반 | 청렴감사팀장(총무과) | 055-772-3140 | hans4@gnu.ac.kr |

### ❍ 협력업체/유지보수업체

| 업체명 | 담당 시스템 | 담당자 | 전화번호 | 이메일 |
|---|---|---|---|---|
| 투썸데이터 | 오라클DB | 강경수 | 010-4568-4957 | gsgang@2sumdata.com |
| 아이웍스 | IBM서버 | 박태영 | 010-3849-3895 | tkpark@iworks.kr |
| 우리아이티 | 네트워크 | 전경인 | 010-5537-5138 | kineon@wooriit.kr |
| 신아시스템 | 방화벽, 보안 | 신동석 | 010-2909-2444 | sindseok@sinasystem.com |
| 네오비트 | 개인정보접속기록 관리시스템 | 유시승 | 010-9138-7803 | yss21@neobit.kr |

# 3 피해 최소화 및 긴급 조치

## 3.1 해킹에 의한 경우

❍ 해킹 등 침해사고 발생으로 인해 개인정보가 유출된 사실을 알게 된 경우에는 개인정보 추가 유출 방지를 위한 대책을 마련하고 피해를 최소화할 수 있는 조치를 강구한다.

- 유출된 시스템 분리·차단 조치, 관련 로그 등 증거자료 확보, 유출 원인 분석, 이용자 및 개인정보취급자 비밀번호 변경* 등 기술적 보호조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 긴급 조치를 시행하여야 한다.

## 3.2 내부자가 유출한 경우

❍ 개인정보 유출자가 개인정보처리시스템에 접속한 이력 및 개인정보열람·다운로드 등 내역을 확인하여야 한다.

❍ 개인정보 유출자의 개인정보처리시스템에 대한 접근·접속 경로 등이 정상적인지 여부 등을 확인하고, 비정상적인 접속인 경우 우회 경로를 확인하여 접속을 차단하여야 한다.

❍ 개인정보취급자의 개인정보처리시스템 접속계정, 접속권한, 접속기록 등을 검토하여 추가적인 유출 여부를 확인하여야 한다.

❍ 개인정보 유출에 활용된 단말기(PC, 스마트폰 등)와 매체(USB, 이메일, 출력물 등)를 회수하고, 필요시 수사기관 등과 협조하여 유출된 개인정보를 회수하기 위한 방법을 강구하여야 한다.

## 3.3 이메일 오발송에 의한 경우

❍ 이메일 회수가 가능한 경우에는 즉시 회수 조치하고, 불가능한 경우에는 이메일 수신자에게 오발송 메일의 삭제를 요청하도록 한다.

❍ 메일서버 외 첨부파일서버(대용량 메일 등)를 이용하는 경우 첨부파일서버 운영자에게 관련 파일의 삭제를 요청하여야 한다.

### 3.4 개인정보 노출에 의한 경우

- ❍ (검색엔진을 통한 노출의 경우) 노출된 사업자의 웹페이지 삭제를 검토하고, 검색엔진에 노출된 개인정보 삭제를 요청하여야 하며, 인증 절차 추가 및 로봇배제 규칙 적용 등 외부 접근을 차단하여야 한다.
- ❍ (시스템 오류로 인한 노출의 경우) 소스코드 오류, 서버 설정 오류 등 개인정보가 노출된 원인이 된 시스템 오류를 파악하여 수정하여야 한다.
- ❍ (개인정보취급자 부주의로 인한 노출의 경우) 게시글 및 첨부파일 내 개인정보 노출 부분을 마스킹 처리하여 게시하도록 한다.

## 4 개인정보 유출 통지 및 신고

### 4.1 개인정보 유출 통지

- ❍ **(통지 시점)** 최초 개인정보의 유출 사실을 알게 되었을 때로부터의 5일 이내을 말한다.
  - 단, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위해 긴급한 조치가 필요하다고 인정되는 경우에는 해당 조치를 취한 후 그로부터 5일 이내에 정보주체에게 알릴 수도 있다
  - 수탁사업자가 수탁 업무를 처리하는 과정에서 개인정보가 유출된 경우 즉시 위탁자에게 보고하도록 위·수탁계약서에 명시하고, 수탁사업자로부터 보고 받은 시점에서 지체없이 유출 통지를 한다.
- ❍ **(통지 규모)** 단 1명의 정보주체에 관한 개인정보가 유출된 경우라 할지라도 해당된다
- ❍ **(통지 방법)** 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법으로 개별 통지하는 것을 말한다.
- ❍ **(통지 내용)**

① 유출된 개인정보 항

② 유출된 시점과 그 경위
③ 정보주체가 취할 수 있는 피해 최소화 조치
④ 개인정보처리자 대응조치 및 피해 구제절차
⑤ 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처

※ 유출 통지하여야 하는 사항 중, 구체적인 내용이 확인되지 않은 경우에는 그 때까지 확인된 내용을 중심으로 우선 통지하고, 추가로 확인되는 내용은 확인되는 즉시 통지하여야 한다.

## 4.2 개인정보 유출 신고

❍ **(신고 시점)** 최초 개인정보의 유출 사실을 알게 되었을 때로부터 5일 이내을 말한다.

❍ **(신고 규모)** 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 신고해야 한다.(개인정보보호법 시행령 제39조제1항)

❍ **(신고 방법)** 개인정보보호위원회 또는 한국인터넷진흥원의 홈페이지, 전화, 팩스, 이메일, 우편 등의 방법으로 신고하여야 한다.

- 이후 홈페이지 또는 사업장에 7일 이상 게시하여야 한다.(이용자의 연락처를 알수 없는 등의 경우에는 홈페이지에 30일 이상 게시)

| 신고 기관명 | 전화번호 | 팩스번호 | 이메일 | 홈페이지 |
|---|---|---|---|---|
| 개인정보보호위원회<br>한국인터넷진흥원 | 118 | 02-405-5219 | 118@kisa.or.kr | 개인정보보호 종합포털 (privacy.go.kr) |

※ 개인정보보호 종합포털 → 민원마당 → 개인정보 유출 침해신고 → 개인정보 유출신고

❍ **(신고 내용)** 정보주체에게 해당 개인정보의 유출 사실을 통지한 결과, 유출로 인한 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 이행한 결과를 말하며 “개인정보 유출 신고서”를 제출해야 한다.

- 유출 신고하여야 하는 사항 중, 구체적인 내용이 확인되지 않은 경우에는 그 때까지 확인된 내용을 중심으로 우선 신고하고, 추가로 확인되는 내용은 확인되는 즉시 신고하여야 한다.

**< 개인정보 유출 신고서 작성 방법 >**

| 유출 신고서 양식 | 작성 방법 |
|---|---|
| ① 유출된 개인정보 항목 | · 유출된 개인정보 항목을 모두 기재해야 하며, '등'과 같이 일부 생략하거나 휴대전화번호와 집 전화번호를 '전화번호'로 기재하여서는 안됨<br>· 유출된 개인정보의 모든 항목을 적어야 하며, 유출 규모도 현 시점에서 파악된 내용을 모두 작성 |
| ② 유출된 시점과 그 경위 | · 유출시점, 인지시점을 명확히 구분하여 날짜 및 시간 모두 작성해야 하며, 유출경위와 인지경위를 포함 |
| ③ 정보주체가 취할 수 있는 피해 최소화 조치 | · 개인정보 유출로 발생 가능한 스팸 문자, 보이스피싱, 금융사기와 같은 2차적인 피해 방지를 위해이용자가 할 수 있는 조치를 기재(예: 비밀번호변경 등) |
| ④ 개인정보처리자 대응조치 및 피해 구제절차 | · 유출사실을 안 후 긴급히 조치한 내용과 향후 이용자의 피해구제를 위한 계획 및 절차를 기재<br>ex) 경찰에 신고, 일시적 홈페이지 로그인 차단 (홈페이지 해킹일 경우) |
| ⑤ 정보주체가 피해 신고. 상담 등을 접수할 수 | · 유출된 기관명, 사업자번호, 사업자 주소, 웹사이트 주소 등 기재 |
| ⑥ 기타 | · 유출된 기관명, 사업자번호, 사업자 주소, 웹사이트 주소 등 기재 |

# 5 피해 구제 및 재발 방지

## 5.1 정보주체 피해 구제

❍ **(유출여부 조회)** 정보주체가 개인정보 유출여부 등을 확인가능하도록 별도의 홈페이지 등을 제공하도록 한다.

- 본인확인 수단으로 핸드폰, 이메일 인증 등을 활용
- 해당 홈페이지를 통하여 추가적인 개인정보 유출이 발생하지 않도록 웹 취약점 제거, 전송구간 암호화 등 안전조치를 이행

❍ **(민원대응)** 개인정보 유출로 인한 정보주체의 피해 신고·접수, 상담·문의 등 각종 민원에 대응한다.

- 개인정보 유출 문의에 신속히 대응할 수 있도록 상담 스크립트를 운영하고 전화, 이메일, 홈페이지, SNS 등 다양한 채널을 통해 개인정보 유출 사실, 경위 등을 확인할 수 있는 창구를 마련.
- 유출 규모와 상황을 종합적으로 고려하여 원활한 민원대응을 위해 민원대응 전담부서 운영.

❍ **(현장혼잡 최소화)** 유출 대응 현장에서의 긴급·돌발 상황 발생 등에 따른 혼란 최소화를 위한 방안을 강구한다.

- 현장에서 물리적 시스템 장애, 파괴 그리고 불필요한 인력 등으로 인하여 개인정보가 분실, 도난, 훼손되지 않도록 주의 하여야 한다.

❍ **(고객불안 해소)** 2차피해 방지를 위한 유의사항을 사전 안내하고 유출·피해 및 대응 현황 등을 실시간으로 정확하고 투명하게 공개하는 등 고객불안 해소를 위해 노력한다.

❍ **(피해구제)** 정보주체의 피해 구제 계획을 마련하고 개인정보분쟁조정 위원회, 손해배상제도 등도 함께 안내한다.

## 5.2 재발 방지 대책 마련

❍ 개인정보 유출 원인, 취약점 등에 적절한 대책을 마련하고 개인정보 취급자 대상 개인정보보호 교육을 정기적으로 실시하여야 한다.

❍ 개인정보 유출 대응 시나리오 작성 및 모의훈련 등을 실시하여 유출 대응 체계를 점검하고 지속적으로 보완하도록 한다.

❍ 홈페이지 취약점 등으로 인한 유출 사고 예방을 위해 안전조치를 강화하도록 한다.

- 홈페이지의 취약점을 연 1회 이상 정기적으로 점검하도록 한다.
- 개인정보가 인터넷 상에 노출되는 것을 방지하기 위해 인증 절차 추가 및 로봇배제 규칙을 적용하여 홈페이지 접근을 제한하도록 한다.
- 홈페이지에 첨부파일을 포함한 게시글 작성시 개인정보 포함 여부를 확인하도록 한다.
- 홈페이지 게시판 등에 정보주체가 글 작성시 개인정보가 노출되지 않도록 주의할 것을 안내하도록 한다.
- 관리자 페이지에 접근하는 IP를 제한하거나 아이디, 비밀번호 외 추가적인 인증수단을 사용하여 접속하도록 한다.

## 붙임 1 유출통지 방법

# 유출통지 방법

| 구 분 | 내 용 |
|---|---|
| 통지대상 | 정보주체 |
| 통지방법 | ○ 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법<br>○ 위의 통지방법과 동시에 홈페이지에 공개하는 것이 바람직<br>- 단, 통지 및 조치 후에도 1천명 이상의 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 7일 이상 통지내용을 게재 |
| 통지내용 | ○ 유출된 개인정보의 항목<br>○ 유출된 시점과 그 경위<br>○ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보<br>○ 개인정보처리자의 대응조치 및 피해 구제절차<br>○ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 |
| 통지시기 | 유출사실을 발견할 때로부터 5일 이내 |
| 통지연기 | ○ 개인정보 유출확산방지를 위한 조치가 필요한 경우 연기 가능<br>- 개인정보가 유출되었을 것으로 의심되는 개인정보처리시스템의 접속권한 삭제·변경 또는 폐쇄 조치<br>- 네트워크, 방화벽 등 대·내외 시스템 보안점검 및 취약점 보완 조치<br>- 향후 수사에 필요한 외부의 접속기록 등 보존 조치<br>- 정보주체에게 유출 관련 사실을 통지하기 위한 유출확인 웹페이지 제작 등의 통지방법 마련 조치<br>- 기타 개인정보의 유출확산 방지를 위한 필요한 기술적·관리적 조치<br>○ 개인정보처리자는 위 각 항목의 조치를 취한 이후, 정보주체에게 다음 각 항목의 사실만 일차적으로 알리고 추후 확인되는 즉시 알릴 수 있음<br>- 정보주체에게 유출이 발생한 사실<br>- 통지내용 중 확인된 사항 |

# 개인정보 유출 표준 통지문안 (예시)

※ 유출된 항목, 유출된 시점과 경위가 확인되지 않아 통지문에 포함하지 않은 경우 추후 확인되면 반드시 추가 통지

| 표준 통지문안 예시 | 부가 설명 |
|---|---|
| 귀하의 개인정보는 ○○○시스템에 저장·보관하다가 ○○○○년 ○○월경 해커에 의한 해킹으로 유출되었습니다. | <유출된 시점과 경위><br>- 유출된 시점과 경위를 상세하게 설명 |
| 유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 주민등록번호, 이메일, 연락처 총 6개입니다. | <유출된 항목><br>- 유출된 항목을 누락 없이 모두 나열 |
| 유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다. | <개인정보처리자의 대응조치><br>- 예시된 항목 외에도 조치한 내용 설명 |
| 혹시 모를 피해를 최소화하기 위하여 귀하의 비밀번호를 변경하여 주시기 바랍니다.<br><br>그리고 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 연락주시면 친절하게 안내해 드리고, 신속하게 대응하도록 하겠습니다. | <피해 최소화를 위한 정보주체의 조치방법><br>- 유출 경위에 따라 정보주체가 할 수 있는 방법을 안내<br>- 예방 가능한 방법을 모두 안내<br>(보이스 피싱, 피싱 메일, 불법 TM, 스팸문자 등) |
| 아울러, 피해가 발생하였거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해드리겠습니다. | <개인정보처리자의 피해 구제절차><br>- 보상이나 배상이 결정된 경우에는 그 내용을 상세히 기재<br>- 감독기관 등을 통한 구제절차도 안내 |
| ▸ 피해 등 접수 담당부서 : 0000과<br>▸ 피해 등 접수 전화번호 : 02-2345-6789<br>▸ 피해 등 접수 e-메일주소 : abcd@efgh.co.kr | <피해 등 신고 접수 담당부서 및 연락처><br>- 전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내 |

## 붙임 2 유출신고서 양식

[별지 제1호 서식]

### 개인정보 유출신고(보고)서

<table>
<tr><td>기관명</td><td colspan="5"></td></tr>
<tr><td>정보주체에의<br>통지 여부</td><td colspan="5"></td></tr>
<tr><td>유출된 개인정보의<br>항목 및 규모</td><td colspan="5"></td></tr>
<tr><td>유출된 시점과<br>그 경위</td><td colspan="5"></td></tr>
<tr><td>유출피해 최소화<br>대책·조치 및 결과</td><td colspan="5"></td></tr>
<tr><td>정보주체가 할 수<br>있는 피해 최소화<br>방법 및 구제절차</td><td colspan="5"></td></tr>
<tr><td rowspan="3">담당부서·담당자<br>및 연락처</td><td></td><td>성명</td><td>부서</td><td>직위</td><td>연락처</td></tr>
<tr><td>개인정보<br>보호책임자</td><td></td><td></td><td></td><td></td></tr>
<tr><td>개인정보<br>취급자</td><td></td><td></td><td></td><td></td></tr>
</table>

| 유출신고접수기관 | 기관명 | 담당자명 | 연락처 |
|---|---|---|---|
| | | | |