문서번호	홍보전산과-4627
결재일자	2015.2.5.
공개여부	대시민공개

★주무관	정보통신담당	홍보전산과장	행정국장
정덕환	주동근	권용대	02/05 손정수
협 조 자	미디어담당 윤성열 정보화운영담당 김재욱		

성북구 개인정보침해사고 대응지침

2015. 2.

행 정 국

홍 보 전 산 과

성북구 개인정보침해사고 대응지침

우리구에서 처리중인 개인정보에 대한 침해사고 발생시 신속하고 효과적인 대응을 통해 피해를 최소화 하여 신뢰받는 구정을 구현코자 함.

Ⅰ 추진근거

○ 개인정보보호법 제34조(개인정보 유출 통지 등)

○ 개인정보보호법 시행령 제39조, 제40조

○ 표준 개인정보보호 지침 제29조(개인정보 유출신고)

Ⅱ 적용범위 및 대상

○ 대　　상 : 성북구청 및 소속기관(직속기관 및 사업소)

○ 적용범위 : 전자적 처리여부를 불문하고 수기문서를 포함한 모든 형태의 개인정보파일을 운용하는 개인정보처리자

Ⅲ 개인정보 침해유형

○ 업무과실로 인한 개인정보 유출

- 개인정보가 포함된 서면, 이동식저장장치, 휴대용 PC 등을 분실하거나 도난당한 경우

○ 외부 침투에 의한 유출

- 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우

○ **개인정보 오남용으로 인한 유출**

- 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 그밖에 저장매체가 권한이 없는 자에게 잘못 전달된 경우

○ **그 밖에 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우**

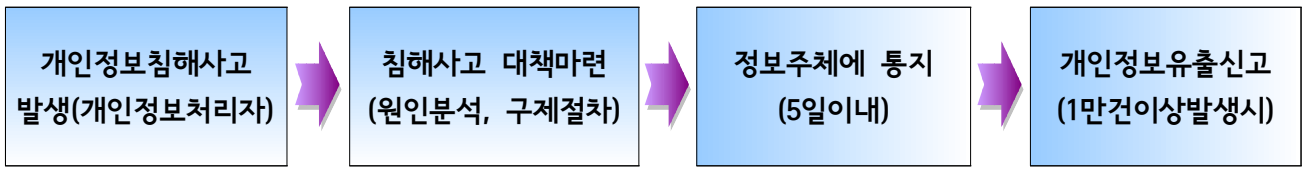
Ⅳ 개인정보 침해사고 대응체계

▢ 개인정보침해사고 대응 조직

- 개인정보보호 책임자 : 개인정보침해사고 대응반 구성
- 침해사고대책반장 : 개인정보침해사고 대응 여부결정
- 총괄 및 사고조사팀 : 개인정보침해사고 상황관리 및 원인분석, 대책마련
- 시스템 조사팀 : 개인정보처리시스템 조사 및 분석
- 개인정보분야별책임자 : 개인정보침해현황 파악 및 상황보고, 사고조사 지원

Ⅴ 개인정보 침해사고 대응절차

▢ 개인정보침해 업무처리 기본절차



<표준 개인정보 보호지침> -- 행정안전부고시 제2011-45호(2011.9.30)

제29조(개인정보 유출신고) ① 개인정보처리자는 **1만명 이상**의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 **5일 이내**에 행정안전부장관 또는 시행령 제39조제2항 각호의 전문기관 중 어느 하나에 신고하여야 한다.

▢ 사고 유형별 대응 프로세스

○ 업무과실로 인한 개인정보 유출

사례1) 업무담당자가 부주의로 개인정보가 포함된 각종파일을 웹사이트에 게재

	개인정보취급자	사고대책반	개인정보책임관
초기 대응	- 개인정보침해 인지 및 침해사실보고(CPO) - 개인정보 침해 범위 파악	- 개인정보 유출 유형 파악 - 해당게시물에 대한 자료수집 및 회수 - 개인정보 침해 여부 판단	- 개인정보침해사고 대책반 구성
본격 조치	-	- 해당 웹사이트에 대한 점검 (개인정보노출검색시스템) - 해당 사이트에 로그분석 - 사고 원인 조사 - 개인정보유출 증거확보 및 보존 - 정보보안시스템을 이용한 보안정책 강화	-

사후 대응	- 정보주체에게 침해사실 통지 - 개인정보피해 구제방안 마련 및 상담	-	- 개인정보침해사실신고(행정자치부) - 개인정보침해사고 재발방지대책 마련 - 법적조치(징계 등)

○ **외부 침투에 의한 유출**

사례2) 접근권한이 없는 자가 해킹을 통해 정보시스템에 접근하여 개인정보 유출

	개인정보취급자	사고대책반	개인정보책임관
초기 대응	- 외부해킹 예상징후 파악 - 해킹시도 공격자 IP차단요청	- 보안시스템을 이용한 침입시도 관련내용 탐지 - 공격 IP 접근차단 - 네트워크 차단 및 로그확보	- 정보보안침해대응센터 가동
본격 조치	- 침해사고로 인한 피해현황 파악 - 해당시스템 서비스 중단	- 데이터 위변조 및 삭제 흔적 분석 - 공격경로 및 원인 조사 - 해당시스템 로그분석 - 해당시스템에 대한 취약점 점검 - 정보보안시스템 정책 강화	- 유관기관과의 공조체계 유지
사후 대응	- 정보주체에게 침해사실 통지 - 개인정보피해 구제방안 마련 및 상담	- 피해시스템에 대한 지속적인 모니터링 실시 - 주변시스템에 대한 전반적인 보안점검 실시	- 개인정보침해사실신고(행정자치부) - 개인정보침해사고 재발방지대책 마련 - 법적조치(징계 등)

○ 개인정보 오남용으로 인한 유출

사례3) 개인정보 취급자가 지인의 부탁 또는 경제적 이득을 목적으로 타인의 이용에 제공하는등 외부로 유출

	개인정보분야별책임자	사고대책반	개인정보책임관
초기 대응	- 개인정보 침해사실 보고	- 개인정보 유출경로 및 범위 파악	- 개인정보침해사고 대책반 가동
본격 조치	- 개인정보에 대한 접근 차단 - 해당 개인정보취급자 신변확보	- 해당 개인정보취급자 PC 및 개인정보처리시스템 접근 내역 확인 - 수시기관의 사고조사 협조	- 유관기관 보고 및 수사기관에 수사의뢰
사후 대응	- 정보주체에게 침해사실 통지 - 개인정보피해 구제방안 마련 및 상담	- 사고내용 전파	- 개인정보침해사고 재발방지대책 마련 - 법적조치(징계 등)

Ⅵ 개인정보 유출통지 및 신고

▢ 개인정보의 유출통지(정보주체)

○ 통지시기 : 유출사고 확인된 때에 정당한 사유가 없는 한 5일 이내

○ 통지항목

- 유출된 개인정보의 항목
- 유출된 시점과 그 경위
- 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보

- 대응조치 및 피해구제 절차

- 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

○ **통지방법**

- 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법

- 이와 함께 홈페이지에 7일 이상 공지

□ 개인정보 유출 피해 최소화를 위한 조치

○ 개인정보처리시스템의 접속권한 삭제 · 변경 또는 폐쇄 조치

○ 네트워크, 방화벽 등 대내외 시스템 보안점검 및 취약점 보완 조치

○ 수사에 필요한 외부의 접속기록 등 증거 보존 조치

○ 정보주체에게 유출관련 사실을 통지하기 위한 유출확인 웹페이지 제작 등의 통지방법 마련 조치

○ 기타 개인정보의 유출확산 방지를 위해 필요한 기술적 · 관리적 조치

□ 개인정보 유출 신고

○ 신고범위 : 1만명 이상의 정보주체에 관한 개인정보 유출시

○ 신고기관 : 행정자치부, 한국정보화진흥원, 한국인터넷진흥원

- 정보주체에 대한 통지 및 조치결과를 5일이내 신고

○ 신고방법 : 개인정보유출 신고서(따로붙임1)에 따른 신고 제출

따로붙임 : 개인정보유출 신고서 1부. 끝.

[따로붙임 1]

개인정보 유출신고서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고접수 기관	기관명	담당자명	연락처