2020년 개인정보보호 자체 추진계획

2020. 3. 26.



제주지방병무청

목 차

Ⅰ. 배경 및 목표 ····· 1

Ⅱ. 개인정보보호 관리체계 및 현황 ····· 2

Ⅲ. 개인정보보호 세부 추진계획 ····· 3

1 자율적이고 책임있는 개인정보보호 활동 ····· 3

2 개인정보보호 실천 생활화를 위한 인식제고 ····· 5

3 개인정보 피해방지 및 최소화를 위한 협력강화 ····· 6

4 정보주체의 능동적 권리보장 및 권익보호 ····· 7

5 개인정보보호 교육 및 지도점검 ····· 8

6 주요 추진일정 ····· 10

Ⅳ. 행정사항 ····· 10

[붙임 1] 침해사고 대응반 구성 및 역할

[붙임 2] 유·노출 유형에 따른 긴급조치 방법

2020년 개인정보보호 자체 추진계획

Ⅰ 배경 및 목표

국민들의 소중한 병역정보 등 개인정보를 취급함에 있어 **관련 규정을 준수**하고 **개인정보 노·유출 사고가 없도록** 개인정보보호 자체 계획을 수립·추진하여 신뢰받는 병무행정 구현

□ 추진배경

○ 내·외부 환경변화 및 지능화·고도화되는 개인정보 침해유형에 따른 유·노출 및 2차 피해 예방을 위한 관리체계 강화

○ 개인정보보호 처리절차 준수를 통한 개인정보 안전성 확보 및 정보주체의 권인보호를 위한 사전·사후 권리보장 강화

○ 개인정보 유출사고를 근절하기 위해 자체 대책 마련

□ 추진목표

○ 신기술로 고도화되는 개인정보보호 위협요인에 선제적 대응

○ 개인정보처리자의 자율적 역량강화 및 정보보호의 안전성 확보

○ 개인정보 취급자의 능동적 정보보호 활동의 생활화

□ 중점 추진 사항

○ 자율적이고 책임 있는 개인정보보호 활동

○ 개인정보보호 실천 생활화를 위한 인식제고

○ 개인정보 피해방지 및 최소화를 위한 협력 강화

○ 정보주체의 능동적 권리보장 및 권익보호

□ 관련법령 및 근거

○ 개인정보 보호법(법률 제14839호) 및 시행령, 시행규칙

○ 표준 개인정보보호 지침(행정안전부고시 제2017-1호)

○ 병무청 개인정보보호 관리규정(훈령 제1677호)

○ 병무행정 정보업무 관리규정(훈령 제1619호)

Ⅱ 개인정보보호 관리체계 및 현황

□ 개인정보의 정의

“개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보화 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

□ 개인정보보호 조직 구성

구 분	개인정보 보호책임자 (CPO)	개인정보 보호분야별 책임자	총괄 개인정보 보호담당자	각과 개인정보 보호담당자	개인정보 취급자
담당자	청 장	각 과장	정보관리계장	각과 개인정보 보호담당자	개인정보를 취급하는 전 직원

□ 개인정보보호 조직 운영

○ 개인정보보호책임자 및 총괄개인정보보호담당자 : 변동 7일내 본청보고

○ 개인정보 보호분야별 책임자 : 별도지정 없이 부서장 자동 임무 부여

○ 개인정보 보호담당자 : 각 부서장이 지정, 변경 시 공문 통보

○ 개인정보 취급자 : 최소한의 범위로 자료접근 권한 부여

□ 개인정보보호 조직의 역할

구 분	임무 및 역할
개인정보 보호책임자 (CPO)	개인정보보호 계획 및 방침의 수립·시행
	개인정보 처리실태 및 관행의 정기적 조사 및 개선
	개인정보 처리와 관련한 불만의 처리 및 피해 구제
	개인정보 유출 및 오·남용 방지를 위한 내부통제시스템 구축
	개인정보파일의 보호 및 관리·감독 등
개인정보 보호분야별 책임자	해당부서의 개인정보 취급자에 대한 개인정보 보호 업무의 지도 및 감독
	개인정보취급자의 업무범위 및 접근권한에 대한 확인·감독
	개인정보처리시스템의 접속기록 분석 및 오·남용 사고의 예방
	그 밖에 해당부서의 개인정보 보호를 위해 필요한 사항 등
총괄 개인정보 보호담당자	개인정보보호 계획 수립·시행 및 개인정보침해 대응
	개인정보처리 실태관리 및 각종 자료 취합, 개인정보보호 교육
	개인정보 보호분야별 책임자가 위임한 개인정보와 관련한 업무
	개인정보처리와 관련한 시스템 연계 등과 관련된 업무 등
개인정보 보호담당자	개인정보보호 자체계획에 의한 부서별 정보보호 업무 수행
	개인정보 보호분야별책임자가 위임한 개인정보와 관련한 업무
	개인정보 처리실태 관리 및 각종 자료 취합 보고
	개인정보처리와 관련된 시스템 연계 등과 관련된 부서업무 등
보호담당자	업무수행 시 처리되는 개인정보에 대한 보호관리
	인터넷 홈페이지에 게재되는 개인정보에 대한 안전한 처리
	CCTV 등 개인영상정보에 대한 보호관리
	개인정보의 열람·정정·삭제 시 보호관리 등

□ 개인정보파일 보유 현황

(2020년 3월, 단위 : 개)

부서명	계	운영지원과	병역관리과
보유건수	30	11	19

□ 영상정보처리기기(CCTV) 설치 현황

(2020년 3월, 단위 : 대)

설치장소	계	민원봉사실	병역판정검사장
설치대수	17	3	9

Ⅲ 개인정보보호 세부 추진계획

1 자율적이고 책임있는 개인정보보호 활동

□ 필요 최소한의 개인정보 수집·이용 문화 정착

○ 필요한 최소한의 개인정보만 수집·처리

○ 고유식별정보 및 민감정보는 별도 동의 및 법령에 의해 처리

○ 개인정보자료 추출 요구 시 필요항목의 구체적 명시 요청

□ 목적 외 이용 및 제3자 제공 시 수집목적 범위 내에서 제공

○ 제공 시 법적근거 확인 및 안전성 확보를 위한 구체적인 조치사항 명시

○ 제공내역 인터넷 홈페이지 등에 공고(10일 이상, 30일 이내)

□ 개인정보처리시스템 자율점검

○ 개인정보처리시스템 자율점검표에 따라 자율점검 실시

○ 자율점검 결과 침해요인 제거 등 개선방안 수립 시행

□ PC내 개인정보 보유자료 관리 철저

○ 과별 개인정보 보유목록 적절성 검토(분기 1회, 부서장 결재)

○ 개인정보검색 프로그램을 활용한 PC내 개인정보 점검

- PC내 개인정보 최소화를 위한 상시 자율 + 일괄 점검체계 확립

- 불필요한 자료 및 보유목적이 종료된 자료 즉시 삭제

② 개인정보보호 실천 생활화를 위한 인식제고

□ 개인정보보호의 날 지정 운영

○ 개인정보보호의 날 : 매월 1일(휴일인 경우 다음날 평일)

○ 개인정보보호의 날 전 직원 동참 유도

- 개인정보 목적 외 열람금지 및 목적달성 개인정보 파기

- 개인용 PC 3단계 암호설정 및 화면보호기 주기적 암호 변경

□ 사이버 보안진단의 날 행사 적극 동참 유도

○ 사이버 보안진단의 날 : 매월 세 번째 주 수요일(전 직원 참여)

- 월별 보안 필수 점검항목 점검 및 '내PC 지키미' 실행

○ 개인정보검색 프로그램 실행 및 PC내 개인정보 관리 철저

□ 개인정보보호 자가진단을 통한 환류 체계 확립

○ 다모아 포털 팝업을 통한 문제풀이(10문항) : 분기 1회

○ 전 직원 문제풀이 후 정답과 해설제공, 오답에 대한 재학습

□ 개인영상정보기기(CCTV) 관리 강화

○ 영상정보처리기기 관리책임자 지정 관리 및 점검(주 1회)

○ 개인영상정보의 보유기간 준수 및 파기 기록관리

□ 개인정보파일 표준목록 정비

○ 개인정보보호 종합지원시스템 개인정보파일 목록 현행화

- 개인정보파일 등록, 항목변경, 파기 등

□ **개인정보의 안전한 활용을 위한 지원 체계 강화**

○ 업무 및 인터넷 PC 보안정책 강화

○ 숨겨진 개인정보 및 악성코드 제거를 위한 전 직원 PC 포맷

- 업무 PC(인사이동 자), 인터넷 PC(전 직원, 반기 1회)

○ 정보화시스템 접근권한 부여 점검

- 자료접근 권한 통제 및 최소 적정 권한 승인 여부

- 시스템 처리로그 현황 모니터링(월 1회)

□ **생활 속 실천을 위한 정보보호 활동**

○ '혼디 손심엉 정보보호 실천' 캠페인 실시

- 정보보호 Day 운영 : 매월 1일

- 소식지 발간(메모보고 이용) 및 구내방송 : 매월 주제 설정

- 정보보호 인식제고 및 직원 관심 유도

- 자리 이석 시 화면 잠금 '키보드 스티커' 제작 배포

○ 개인정보보호 홍보 강화

- 개인정보보호 10계명 화면보호기 제작 배포

- 개인정보 Q&A 및 정보보호 사고 사례모음집 제작

□ **개인정보보호 정보공유(개인정보 지킴e) 게시판 활용**

○ 각종 법령, 매뉴얼, 교육자료, Q&A 적극 활용

○ '개인정보관련 트렌드' 전 직원 공유(메모보고 활용)

3 개인정보 피해방지 및 최소화를 위한 협력 강화

□ **개인정보 유·노출 대응강화**

○ 개인정보 유·노출 예방을 위한 모의훈련 실시 : 반기 1회

○ 업무자료 '바로톡' 사용, 자료 반출시 사전결재 등 보안강화

○ 개인정보 유·노출 및 침해사고 사고 대비 대응반 운영(붙임1)

□ 홈페이지 개인정보 노출 방지를 위한 모니터링

○ 홈페이지 자료 게재 시 개인정보 포함여부 확인 절차 준수

○ 홈페이지 개인정보 모니터링 담당자 지정 및 점검(1일 2회)

□ 재해·재난 대비 개인정보처리시스템 위기대응 강화

○ 개인정보처리시스템의 위기발생 시 피해 최소화 및 신속한 복구

○ 재해·재난 대비 개인정보처리시스템 위기대응 모의훈련(연 1회)

- 본청과 협의 후 병무행정시스템 위기대응 종합훈련과 병행 실시
- 재해·재난 등에 대비한 병역정보의 안전한 보호를 위한 모의훈련
- 위기 발생 시 피해를 최소화하고 신속한 복구 체제 운영

※ 세부내용은 “재해·재난 대비 개인정보처리시스템 자체 위기대응 계획” 참조

○ 위기발생 대비 예방점검

- 장애 사전 예방을 위한 시스템 상시 모니터링
- 시스템 관제 솔루션을 통한 장비별 이상 유무 점검
- 주기별 백업 체계 유지 : 복제 솔루션 OGG 확인 및 점검(매일)

4 정보주체의 능동적 권리보장 및 권익보호

□ 개인정보 자기결정권 실질화

○ 정보주체 권리행사 시 지원을 위한 기반 마련

- 권익구제 상담, 침해유형 등 사례관리 및 전파
- 개인정보처리방침 변경 사항 반영 및 이력 관리

○ 개인정보 수집·이용·제공 관련 동의사항 적정성 검토

□ 개인정보 침해신고 대응체계 마련

○ 개인정보 침해 신고처 체계적 관리 및 운영

- 개인정보 침해 신고처 : 개인정보 보호담당자
- 권익구제 상담, 침해유형 등 사례관리 전파
- 정보주체 개인정보 침해유형 사전 점검 및 제거

○ 개인정보침해 신고센터

- 개인정보보호 침해신고 문의 : (국번없이) 118
- 신고방법 : www.privacy.go.kr 접속 → 민원마당 → 개인정보 유출신고 화면에서 입력

○ 개인정보보호 침해 모니터링

- 홈페이지 등의 개인정보 유·노출에 대한 상시 모니터링
- 인터넷 망으로 자료 반출 시 사전결재 및 상급자 승인
- PC내 개인정보 관리실태 지속적 모니터링 및 결과 공유
- 자료접근 권한 통제 및 최소 적정 권한 승인여부

⑤ 개인정보보호 교육 및 지도점검

□ 개인정보보호 교육

○ 교육대상별 맞춤형 교육 실시로 효과성 제고

- 개인정보 보호책임자(CPO)의 관심·역량 강화
  · 행안부 주관 개인정보 보호책임자(CPO) 워크숍 1회 이상 참석
  · 개인정보보호 관련 최신이슈·환경변화, CPO 역할 등 공유
- 개인정보보호 지정강사 전문성 향상
  · 전문성 향상을 위한 전문교육 과정 연 1회 이상 의무 이수
- 개인정보보호 담당자 업무역량 강화
  · 본청(대전) 주관 개인정보보호 직장교육 의무 참석(연 2회)
- 개인정보 취급자 및 일반직원 기본원칙 숙지
  · 외부 교육기관 교육과정(집합, 이러닝) 1과목 이상 이수
  · 개인정보보호 교육 연 2시간 이상 이수
- 사회복무요원에 대한 개인정보보호 중요성 인식
  · 개인정보 유출사례 중심 교육

- 외부 용역업체 수탁자(직원) 관리·감독 및 교육

· 위탁업무 내용에 맞는 수탁지원 교육(반기 1회)

· 위탁 범위 내에서 개인정보 분실·도난·유출·위조·변조·훼손 방지를 위한 개인정보 안전성 확보 중심 교육

❍ 개인정보보호 자체 직장교육

- 전 직원 집합교육 : 연 2회(전·하반기)
- 신규직원(실무수습 포함) 교육 : 사유 발생 시
- 복직직원(2년 이상 휴직자) 교육 : 복직 시

* 신규직원 및 복직 직원은 집중교육 실시(지정강사 교육실시)

- 사회복무요원 교육 : 연 1회 이상

□ 개인정보보호 지도점검

❍ 개인정보보호 자체 지도점검

- 지도점검 방법 및 시기

· 점검방법 : 시스템 점검 및 현장점검 병행

· 점검시기 : 연 2회(전·하반기)

· 점검반 편성 : 정보관리계장 외 개인정보보호 담당

❍ 지도점검 주요내용

- 기본에 충실한 개인정보보호 점검항목에 의한 자율점검
- 취약분야 점검 및 상시 모니터링, 개인정보보호 활동 강화
- 개인정보보호 인식확산 및 소통활성화를 통한 역량강화
- 결함사례 위주의 점검으로 동일한 결함사례 방지
- 취약분야 집중점검 사항

· 개인용 PC내 개인정보 파일 보관 적정여부

· 개인정보의 목적 외 이용 및 제3자 제공 시 안전성확보 여부

· 개인정보처리업무 위탁 시 관리·감독 및 교육 여부

6 주요 추진일정

구 분	1분기			2분기			3분기			4분기		
	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월
개인정보보호 자체 직장교육					■					■		
위탁업체(수탁자) 개인정보 교육	■						■					
개인정보보호 자체 지도점검					■					■		
개인정보 유·노출 모의훈련						■			■			
재해·재난대비 위기대응 훈련									■			
개인정보보호 자가진단			■			■			■		■	
개인정보파일 목록 현행화			■									
CCTV현황 시스템 등록			■									
PC내 개인정보목록 적절성 검토	■			■			■			■		
홈페이지 개인정보 점검	■	■	■	■	■	■	■	■	■	■	■	■
개인정보보호 보호의 날	■	■	■	■	■	■	■	■	■	■	■	■
사이버보안 진단의 날	■	■	■	■	■	■	■	■	■	■	■	■
혼디 손심엉 정보보호 활동	■	■	■	■	■	■	■	■	■	■	■	■

Ⅳ 행정사항

□ 개인정보보호 교육 및 행사 적극 참여

○ 개인정보보호 및 정보보안 직장교육 적극 참석

- 최소 근무인원 제외한 전 직원 교육 참석
- 미참석시 외부 교육기관 이러닝 교육 이수

○ 개인정보보호의 날 및 사이버 보안진단의 날 적극 참여

- 개인정보보호의 날 : 매월 1일
- 사이버 보안진단의 날 : 매월 세 번째 수요일

○ 개인정보보호 자가진단 전 직원 참여 협조

- 개인정보보호 자가진단 : 3월,6월,9월,11월 마지막주 월~화요일

○ 개인정보보호 종합포털 온라인 교육 수강

- 교육마당 → 온라인 교육(http://www.privacy.go.kr)

- 대상 : 개인정보취급자 및 일반직원 등

□ 강조사항

○ 개인정보 수집 시 법령 및 동의절차를 준수하여 개인정보 처리

○ 개인정보 위탁업체(수탁자) 관리·감독 및 교육 철저

○ 홈페이지 자료 게시 시 반드시 개인정보 포함여부 확인

○ 개인정보 자료 조회 및 제공 시 정확한 법적근거 확인 및 자료의 안전성 확보조치(최소한의 범위로 한정)

□ 행정사항(각 과)

○ 개인정보검색 프로그램을 활용한 PC내 개인정보 관리 철저

- PC내 개인정보 최소화를 위한 상시 자율 점검체계 생활화

○ 과별 개인정보 보유목록 적절성 검토(분기 1회, 부서장 결재)

○ 개인정보포함 자료추출 요구 시 필요항목 구체적 명시

○ 병무행정 업무관련 기관 교육 시 개인정보 교육 및 공문 명시

- 내용 : 개인정보 안전성 확보 조치 등

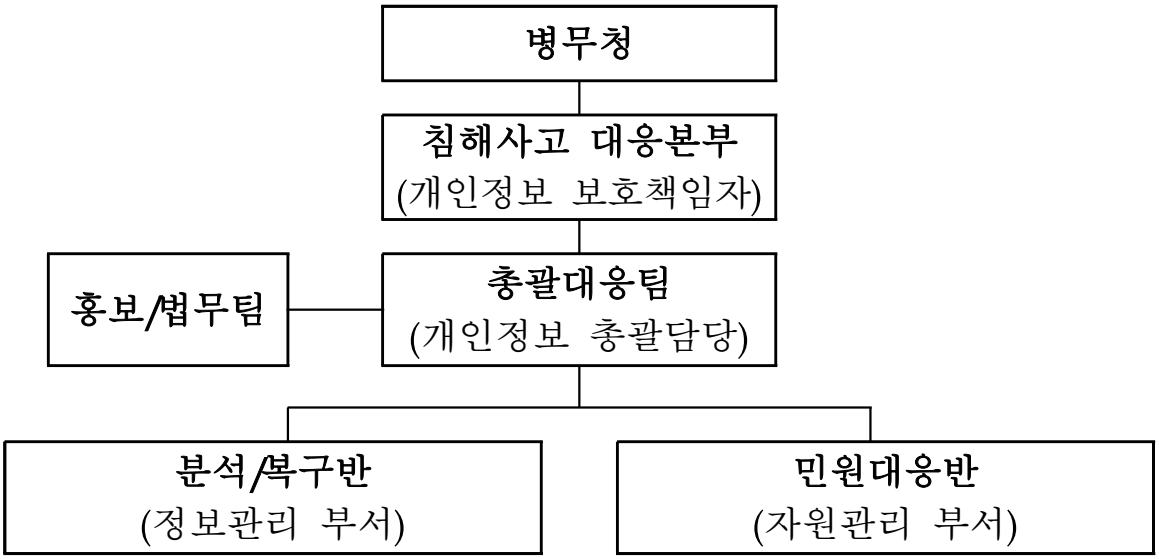
* 개인정보가 포함된 문서 기안 시 열람범위(열람불가) 및 비공개 조치

○ 인터넷망으로 자료전송 시 반드시 승인권자 사전결재

○ 업무관련 자료는 '바로톡' 사용

붙임 1 침해사고 대응반 구성 및 역할

□ 조직구성(침해사고 대응반)



□ 업무분장

조직별	담당자	담당업무
병무청	병무청장	▸ 사고종료 시까지 제반사항 최종 의사결정
침해사고 대응본부	개인정보 보호책임자	▸ 대상 : 지방청장 ▸ 유출사고 대응 총괄 지휘
총괄대응팀	총괄 개인정보 보호담당자	▸ 본청과 소속기간 개인정보담당자 간 협조체계 ▸ 유출사고 접수, 확인, 전파 및 원인 분석 ▸ 유출사고 대응 절차 수립 ▸ 행정안전부 또는 점문기관에 유출통지 사실 신고
분석/복구반	정보관리부서	▸ 사고내용 세부조사 ▸ 외부요인 유출 시 유관기관 협조로 사고처리 지원 ▸ 시스템 복구 및 백업(유지보수/협력업체 포함)
민원대응반	자원관리 부서	▸ 정보주체에게 유출사실 통지 ▸ 고객 개별 통지문 안내에 따른 후속업무(민원 등)
홍보/법무팀	홍보감사계/ 서무계	▸ 유출사고 관련 대외기관(언론사 등) 대응 ▸ 유출사고 대고객 안내문 문구 최종 검토 ▸ 법률상 대응방안 검토의뢰 및 결정

붙임 2 유·노출 유형에 따른 긴급 조치 방법

□ 홈페이지를 통한 유·노출 조치 방법

유형	내 용	긴급 조치방법
웹 페이지 노출	공지사항 등에 개인정보가 포함된 경우	해당 페이지를 즉시 삭제하거나 해당 개인정보 일부를 *로 변환
	민원인이 게재한 글에 개인정보가 포함된 경우	민원인의 동의를 거쳐 해당 페이지를 즉시 삭제하거나 해당 개인정보 일부를 *로 변환
	현재 운영되지 않는 홈페이지에 개인정보가 노출되어 있는 경우 - 개인정보가 장기간 노출될 수 있음	웹 서버 내에 사용하지 않는 홈페이지를 모두 삭제하거나 개인정보 노출여부를 일제히 점검하여 삭제 처리
	답글에 개인정보가 포함된 경우	해당 페이지에 포함된 개인정보를 즉시 삭제 후 재 게시
	입력/수정 화면에 개인정보가 포함된 경우 - 웹 페이지의 접근권한 및 인증 등의 설계 오류	홈페이지의 접근권한 관련 보안기능이 어떻게 설계 되었는지를 파악하여 각 웹 페이지별로 접근권한에 따른 정확한 인증절차를 준수하도록 수정
첨부 파일 노출	첨부파일을 열면 개인정보가 노출되는 경우	해당 첨부파일을 먼저 삭제한 후 게시글을 삭제하거나, 개인정보를 제거한 파일을 다시 업로드
	엑셀 파일의 경우 - 다른 Sheet에 개인정보가 포함 - 시야밖에(셀 최하단 또는 최우측 등) 개인정보 위치 - 불완전한 숨김 처리 - 이미지를 덮어씌운 경우 - 치환함수(LEFT함수 등)를 이용한 * 로 변환	해당 첨부파일을 먼저 삭제한 후 게시글을 삭제하거나, 개인정보를 제거한 파일을 다시 업로드
소스 코드 노출	웹 페이지의 게시물에 대한 구분자로서 게시자의 개인정보를 이용하는 경우, 소스코드에 개인정보가 포함	웹 페이지를 구별하기 위해 이용되는 개인정보를 해쉬 함수 등 함수를 이용하여 변환

유형	내 용	긴급 조치방법
	웹 페이지 주소(URL)에 개인정보가 포함된 경우	웹 페이지와 관련된 새로운 주소부여 체계를 적용 또는 웹 페이지 주소(URL)에 이용되는 개인정보를 해쉬함수 등 함수를 이용하여 변환
	웹 페이지 소스코드 파일명에 개인정보가 포함된 경우	해당 파일의 이름을 모두 개인정보와 무관한 파일명으로 변경
외부 검색 엔진 노출	검색엔진에 개인정보가 노출되는 일반적인 경우	- 개인정보가 포함된 웹 페이지 즉시 삭제 - 검색엔진이 수집한 개인정보가 삭제되도록 검색포털 사이트에 요청 ※ 홈페이지 가이드라인 참고
	개인정보가 포함되어 있는 웹 페이지는 삭제되었으나, 구글 검색엔진에 저장되어 검색 시 개인정보가 발견되는 유형	- 특정 디렉터리 리스팅 방지 설정 : UNIX/LINUX, 윈도우 IIS ※ 홈페이지 가이드라인 참고 - 검색엔진이 수집한 개인정보가 삭제되도록 검색포털 사이트에 요청

□ 개인정보 유출

유형(설명)	긴급 조치방법
내부 직원에 의한 고의적인 유출	- 유출된 자료 회수(삭제) 및 추가 유통 방지 - 유출된 자료가 인터넷에서 검색되는지 여부 점검 후 삭제 - 유출된 자료 타인 또는 업체에 판매 등 불법거래 확인 및 신고
개인용컴퓨터(PC)의 관리전환에 따른 유출	
외주용역 사업자에 의한 유출	
전산출력물에 의한 유출	- 유출된 자료 회수(삭제) - 전산출력물의 우가 유통여부 점검 및 삭제

□ 개인정보 사이버 침해사고

: 병무청 사이버 침해사고 대응 계획에 따라 조치