

- ▣ 개인정보 침해 대응 모의훈련을 통해 개인정보의 추가유출 방지 및 대응과정을 점검하고, 실제상황에서 보다 신속하고 체계적인 대응을 통해 피해를 최소화할 수 있도록 조치하고자 함

## □ 훈련개요

- 일 시 : 2022년 12월 21일 14시 00분
- 장 소 : 정보통신센터 및 개인정보보호팀 상황실
- 참석자 : CPO, 정보통신센터, 개인정보보호팀, 총무팀

## □ 훈련내용

- 정보보안 담당자가 접속기록을 관리하던 중 ‘개인정보 처리 시스템’에 접근 권한이 없는 자에게 권한이 부여된 것을 발견하고, 개인정보 다운로드 및 열람내역을 추적하여 개인정보 유·노출이 없는지 확인하는 상황을 가정하여 훈련 실시
- 사고발생부서

사고인지	현황파악	유출신고	유출통지	통지결과보고
<ul style="list-style-type: none"> <li>• 개인정보보호팀 정보보안 담당자가 매달 시행하는 접속 권한 점검 중 ‘학사 정보’ 권한이 없는 박00 선생에게 해당 권한이 주어진 것을 발견함</li> <li>• 열람내역을 추적해 보니 박00 선생이 개인정보를 열람한 내역이 발견 됨</li> <li>• 개인정보보호팀에서 정보통신센터 담당자 및 팀장에게 통보 후 비상상황실 가동함</li> </ul>	<ul style="list-style-type: none"> <li>• 권한부여 일시 및 열람 내역 확인</li> <li>• 위계나 고의로 인한 권한 부여 여부 조사</li> </ul>	<ul style="list-style-type: none"> <li>• 개인정보보호 책임자(CPO)에게 신고</li> </ul>	<ul style="list-style-type: none"> <li>•처리 시스템 본인 정보 열람으로 유출 사항 및 변조 해당 없음</li> </ul>	<ul style="list-style-type: none"> <li>• 해당없음</li> </ul>

○ 생활관 시간대별 훈련 내용

	훈련항목	훈련 시행 내용
13시 57분	사고인지	<ul style="list-style-type: none"> <li>개인정보보호팀 정보보안 담당자가 개인정보보호법 29조에 의거해 접근 권한 관리를 하던 중, 학적 조회 권한이 없는 박00 선생에게 '학사 정보' 권한이 부여됐고, 개인정보 열람 내역을 확인함.</li> <li>정보통신센터 권한 부여 담당자에게 즉시 잘못된 접속 권한 말소를 요청하고 개인정보보호팀에 해당 내용을 보고 함</li> </ul>
14시 10분	현황파악 및 초동조치	<ul style="list-style-type: none"> <li>개인정보보호팀에서는 유출 사고 대응팀을 설치하고 정보통신센터에 내방함. 정보 보안 담당자에게 박00선생의 권한 부여 일자, 열람 내역, 프로그램 리포트 다운로드 기록을 요청함.</li> </ul>
14시 40분		<ul style="list-style-type: none"> <li>상황 파악 결과 위계나 고의로 인한 접근 권한 부여가 아님을 확인하였음. 접근 권한은 정보통신센터 담당자의 업무상 실수로 발생하였음.</li> <li>박00 선생은 접속 권한이 있음을 발견하고 본인의 정보를 열람함. 본인 정보 변조한 내역은 없었으며, 타인의 개인정보에는 접근하지는 않았음을 확인함.</li> </ul>
14시 45분	최종 처리	<ul style="list-style-type: none"> <li>본 사건은 유출통지할 내용은 없음. 개인정보 보호법 시행령의 과태료나 과징금에 해당할 만한 사항은 아니며, 정보보안 사고자 처리 기준에도 중징계 사항에 해당하지 않아 담당자에게는 경고 조치하고, 박00 선생에게는 사유서를 받는 것으로 처리하고자 함.</li> </ul>

○ 개인정보보호팀

사고접수	확인조사	추가피해여부 확인	유출통지 신고
<ul style="list-style-type: none"> <li>사고 접수 후 유출 사고 대응팀 설치</li> </ul>	<ul style="list-style-type: none"> <li>유출 경로 및 권한 내역 확인</li> <li>개인정보 유출 여부 확인</li> </ul>	<ul style="list-style-type: none"> <li>위계나 고의로 인한 접근 권한 부여 여부 확인</li> </ul>	<ul style="list-style-type: none"> <li>해당 없음</li> </ul>

○ 개인정보보호팀 시간대별 훈련 내용

	훈련항목	훈련 시행 내용
14시 10분	사고접수	개인정보 유출 사고 대응팀 설치
14시 15분	확인조사 및 추가피해여부 확인	대응팀에서 정보통신센터에 내방하여 사건 조사 실시
14시 25분		대응팀에서 노출 경위 및 내역 확인
14시 35분		CPO에게 피해 상황 보고 및 추가 유출 확인 후 조사 내용 브리핑
14시 40분		정보보안 사고자 처리 기준 여부 확인, 사법처리 관련 내용 확인
1월 11일	사례전파	부서 교육 후 결과 보고서 작성 후 전파

## 개인정보 유·노출 관련 조사 체크 List

사 고 일 시	2022년 12월 21일(수) 오후 2시
사 고 장 소	정보통신센터 및 행정동 사무실
사 고 내 용	개인정보 접근 권한이 없는 자에게 권한이 주어짐
사 고 원 인	1. 접근 권한 부여 업무 담당자의 실수 2. 권한 부여받은 자의 고의적 열람, 잘못된 권한 인지 후 해당 부서에 미고지

### ○ 개인정보보호 점검 List

구분	번호	세부점검항목	조사결과
내부관리계획에 근거한 문제점 점검	1	개인정보 수집 경로	개인정보 처리시스템
	2	개인정보 수집의 법적 준수 여부	개인정보 수집 및 활용 동의서 받고 있음
	3	개인정보 활용 목적	개인정보 처리시스템 내 학생 관리
	4	유(노)출된 개인정보 주체 수	1건
개인정보 수집에 관한 문제점 점검	5	유(노)출 파일 생성 시기	2013년 2월
	6	유(노)출 파일 생성자	학사정보 담당자
	7	유(노)출 파일 생성 근거	법령 및 정보주체 동의
	8	유(노)출된 개인정보 항목	학번, 이름, 연락처, 주소, 성적 등
개인정보보호를 위한 안정성 확보조치 점검	9	유(노)출 파일 접근 권한자	담당자
	10	유(노)출 파일 사용자	담당자
사건발생 후 조치에 대한 적절성 점검	11	사고대응매뉴얼 준수여부	사건 발생 후 즉각 조치가 잘 이루어짐
총평			1. 정보 보안 담당자가 개인정보보호법 29조에 의거하여 매달 개인정보 접속기록을 잘 보관, 관리하고 있음. 2. 접근 권한 부여 담당자에게는 '접근 권한 부여 프로그램'을 개선하여 사번, 이름, 부서까지 확인할 수 있도록 항목을 수정하여 사용하도록 권고 3. 불법, 고의, 위계에 의한 권한 경우 외에도 편의를 위해 접속 권한을 요청하는 경

구분	번호	세부점검항목	조사결과
			우가 있음. 이는 2023년 개인정보보호법 위반사항임을 알리고, 혹 부서 내 업무 변동 및 잘못된 권한 부여 시 정보통신센터 담당자에게 고지할 것을 직원 교육에 추가하기로 함.

- 정보보안 점검 List
  - 해당없음

## ☐ 훈련결과

- 유출 사고 대응팀이 세분화되어 있어 현장 방문 및 접속기록 확인이 잘 이루어졌으며, CPO가 직접 사고 처리 절차를 지휘하여 체계적인 훈련이 될 수 있었음
- 개인정보보호법 29조에 의거하여 매달 체계적으로 접속기록을 보관, 관리하고 있음. 잘못된 권한부여 내용을 확인 후 매뉴얼에 따라 초동조치가 체계적으로 잘 이루어졌음

## ☐ 개선조치 사항

- 사고 발생 부서 - 접근 권한 부여를 위해 대상자를 선택할 때 사번, 이름 외에 부서명을 추가하여 사용하도록 권고
- 2023학년도 직원 개인정보보호 교육 시 접근 권한 내용 강조하여 교육
- 외부 기관 및 기업에서 권한을 오·남용하여 개인정보 유출 사고 및 변조까지 이어진 사례가 있음. 최근 교육부 및 개인정보보호위원회에서 개인정보 처리시스템 접속 권한 부분을 유의, 주시하고 있으니 더 철저히 관리할 것

☐ 훈련사진

