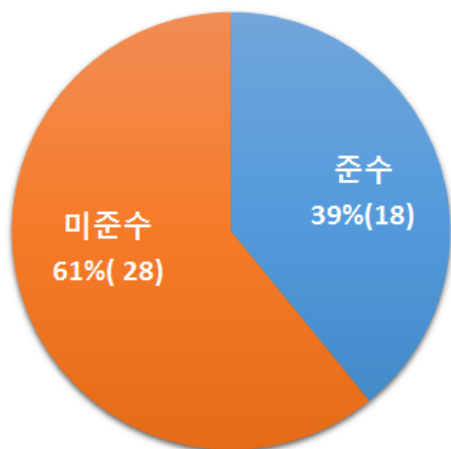
 정보화사회실천연합 <small>ONLINE</small>		보도자료	
보도일시	2016. 07. 22.(금) 조간(온라인 07. 21. 14:00)부터 보도하여 주시기 바랍니다		
배포일시	2016. 07. 21.(목) 09:00	총 8쪽(붙임 6쪽 포함)	
담당부서	개인정보보호 (070-7797-2583)	작 성 자	손영준 (010-8677-9515)

대학들의 개인정보보호는 낙제점

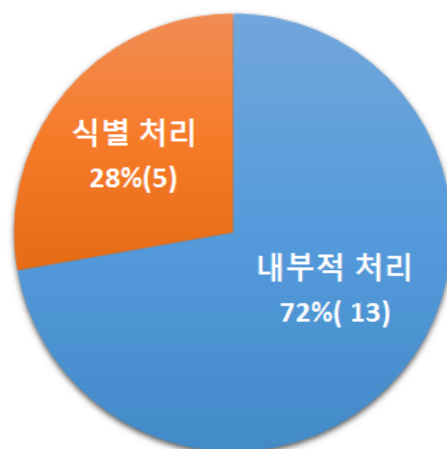
- 대학 61%가 학생들 개인정보보호에 무관심 -

- 서울소재 대학 46곳에 대하여 대학들이 학생들의 개인정보보호에 얼마나 잘 보호하고 있는가에 대하여 실태조사를 하였다. 그러나 대학들의 개인정보보호 준수율은 39%로 낙제점으로 나타났습니다. 특히 이름만 들어도 알만한 대학들조차 미준수하고 있는 것으로 확인되었다.
- 또한 법을 준수한 대학이 이용자를 위하여 안전성조치를 확인할 수 있도록 처리한 대학은 5곳에 불과하여 아직도 안전성확보조치를 이용자의 편의성을 무시하고 내부적 처리를 하고 있어 이용자는 내정보가 안전하게 처리되는지를 확인할 수 없도록 하고 있다.

개인정보 안전성확보 조치 미준수율



안전성확보 조치 식별 처리율



- 개인정보보호법은 개인정보를 처리하는데 있어 기본적인 조치사항으로 안전성을

확보하도록 하고 있으나 이를 준수하지 않고 개인정보를 처리하고 있었다.

○ 개인정보보호법은 개인정보를 처리함에 있어 이용자의 개인정보를 안전하게 처리하도록 규정하고 있으며, 이를 위반 시 과태료를 부과하는 행정조치를 취하고 있다.

○ 금번 조사는 “제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”를 미준수한 사례에 해당 된다.

□ 금번 조사결과를 비추어 보아 전국 대학들의 개인정보보호 수준들로 낙제점으로 볼 수 있으며, 우리의 개인정보 보호 인식 수준의 현주소가 아닌가 합니다 또한 대학을 관리 감독하는 교육부는 이들 대학에 대하여 적절한 조치를 취하여 할 것이다.

□ 이러한 여건에서 지난달 정부는 빅데이터 활성화를 위해 “개인정보 비식별화 조치 가이드라인”을 발표했는데, 비식별화 방법 및 적정성을 평가하는 k-익명성 등의 방법으로는 재식별화를 방지하는데 충분하지 못하며, 또한 개인정보의 정의부터 무조건적 활용을 조장하고 있다. 이는 개인정보를 판매하는 것의 합법화 및 과도한 정보 수집을 조장하는 조치로 개인정보보호법 제18조(개인정보의 목적 외 이용·제공 제한)를 무력화하는 조치로서 행정자치부가 개인정보보호 주무부처로서의 역할을 포기한 행동으로 개인정보보호가 뒤로 퇴보하는 행보를 보이고 있다.

-끝-

□ 붙임

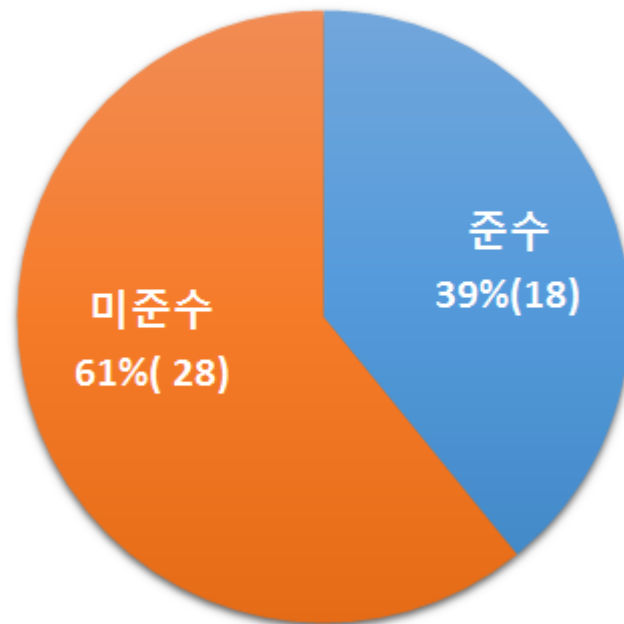
1. 개인정보의 안전성확보 조치(암호화) 조사결과
2. 개인정보보호법 일부
3. 개인정보보호 캠페인 자료

붙임 1

개인정보의 안전성확보 조치(암호화) 조사결과

- 목적 : 본 모니터링은 정보주체가 제공하는 개인정보에 대하여 정보이용자가 관련 법에 따라 안전하게 처리하는가를 확인하여, 개인정보의 유출을 사전에 예방하고자 한다.
- 대상 : 법 "제29조(안전조치의무)"는 안전성 확보에 필요한 기술적·관리적 및 물리적 조치로서, 이는 외부에서 정보수집자의 개인정보보호 수준을 가늠할 수 있는 유일한 방법이다.
- 방법 : 패킷 분석 도구인 와이어샤크(Wireshark)를 이용하여 해당 웹 페이지에 임의의 테스트 정보를 입력하여 전송된 패킷을 분석하여 암호화 여부를 확인.
- 일자 : 2017년 07월

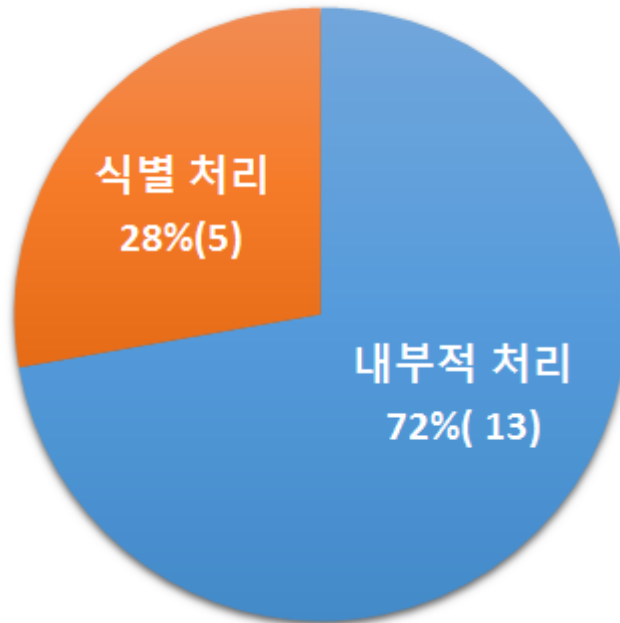
개인정보 안전성확보 조치 미준수율



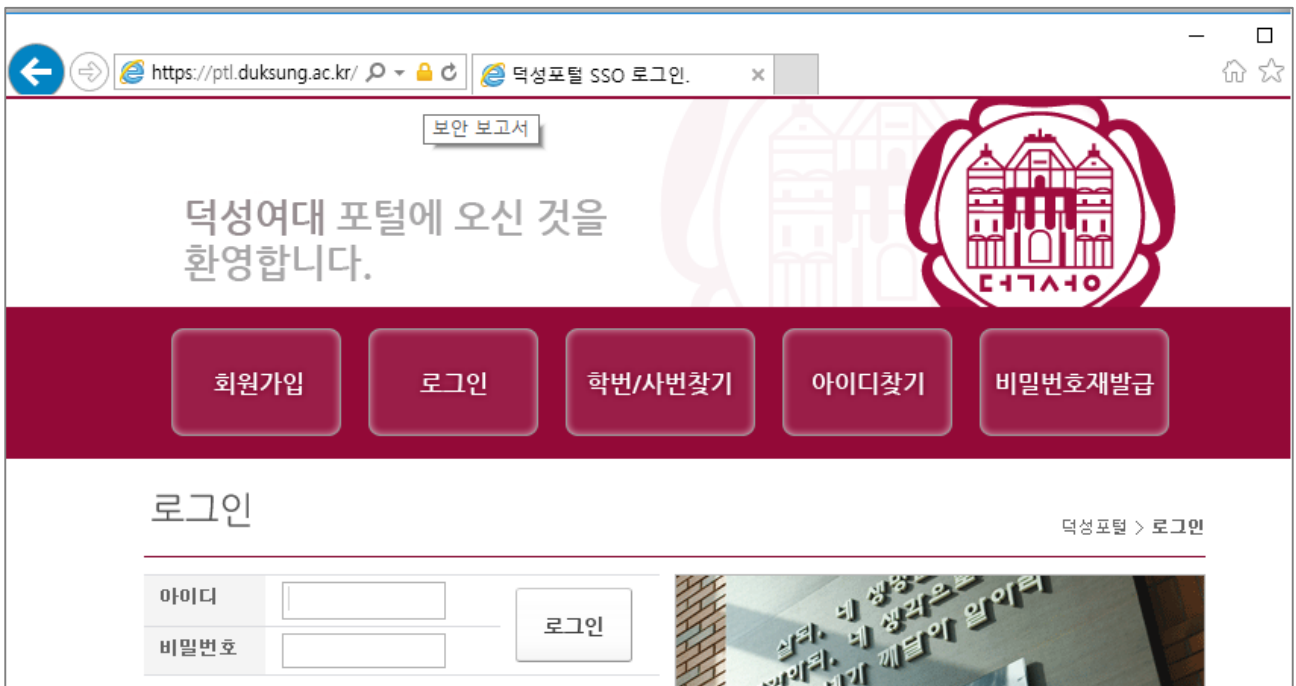
< 대학(서울소재)들의 개인정보 안전성확보조치 미준수율 >

개인정보 보호는 안전한 정보 사회의 기본이다.

안전성확보 조치 식별 처리율



< 준수 대학들 중 이용자를 고려한 식별처리율 >



< 이용자를 고려한 식별처리 모범 사례 >

- 식별처리의 필요성 : 개인정보 안전성 확보 식별처리는 이용자의 개인정보를 처리하는 웹 페이지에 해당 정보를 안전하게 기관 공인인증서를 통하여 암호화하여 처리하고 있다는 표시며, 또한 개인의 공인인증서와 같이 기관의 신분을 확인시켜주는 역할을 하여 해당 사이트가 가짜 웹사이트가 아니라는 표시이기도 하다.

붙임 2

개인정보보호 관련 법

■ 개인정보 보호법 [시행 2016.1.1.] [법률 제13423호, 2015.7.24., 일부개정]

제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

③ 개인정보처리자는 제2항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

④ 공공기관은 제2항제2호부터 제6호까지, 제8호 및 제9호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 행정자치부령으로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다. <개정 2013.3.23., 2014.11.19.>

⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한

개인정보 보호는 안전한 정보 사회의 기본이다.

사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다. [제목개정 2013.8.6.]

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다. <개정 2015.7.24.>

■ 개인정보 보호법 시행령 [시행 2016.1.1.] [대통령령 제26776호, 2015.12.30., 일부개정]

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

② 행정자치부장관은 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다. <개정 2013.3.23., 2014.11.19.>

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정자치부장관이 정하여 고시한다. <개정 2013.3.23., 2014.11.19.>

제63조(과태료의 부과기준) 법 제75조제1항부터 제3항까지의 규정에 따른 과태료의 부과기준은 별표 2와 같다.

[별표 2] <개정 2015.12.30.> 과태료의 부과기준(제63조 관련)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회이 상 위 반
타. 법 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1200	2400

■ 개인정보의 안전성 확보조치 기준 [시행 2014.12.30.] [행정자치부고시 제2014-7호]

제6조(개인정보의 암호화) ① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

개인정보 보호는 안전한 정보 사회의 기본이다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

2. 위험도 분석에 따른 결과

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

붙임 3

개인정보보호 캠페인 자료

“자물통 그림”은 개인정보가 안전하게 처리되고 있다는 “안심식별표시”입니다.

1 주소 창에서 암호화 통신 주소 https:// 를 확인

2 접속사이트 정보를 확인 할 수 있는 자물통을 확인

3 자물통 마우스로 클릭

4 인증서 보기를 통하여 웹 사이트 진위여부를 확인

웹 사이트 ID

GPKIRootCA1 에서 이 사이트를 확인한 결과:
www.open.go.kr
서버에 대한 연결이 암호화되었습니다.
신뢰할 수 있는 사이트

인증서 보기

 해킹 방지 데이터 암호화로 해킹 사전차단 기업 신뢰도 향상	 정보유출 방지 개인정보 암호화 전송으로 개인정보 유출 방지	 위조사이트 방지 사이트 운영자 확인 발급으로 위변조 사이트 사전 확인	 데이터변조 방지 해커의 인위적 데이터 변조 방지로 신뢰된 금융거래 가능
--	--	--	---