

교육일시	2013. 4. 8(월) 14:00~17:00
교육장소	인천광역시교육청 대회의실

The **Good** Edu-Partner
 참 좋은 교육파트너, 인천교육청



2013년 상반기 정보보안 및 개인정보보호 교육



인천광역시교육청
 INCHEON METROPOLITAN CITY OFFICE OF EDUCATION
(정보지원과)

목 차

□ 정보보안 및 개인정보보호 업무 추진 안내	1
I. 인천교육종합정보센터 정보보안시스템 현황	2
II. 정보보안 추진 계획	4
1. 인천광역시교육청 정보보호 관리체계	4
2. 인천광역시교육청 정보보안 기본지침 개정 안내	6
3. 정보공유 및 침해대응시스템 운영	8
4. 정보화사업 보안성 검토 절차	11
5. 무선랜 보안관리	17
6. 정보화사업 용역업체 보안관리 강화대책	19
7. 정보보호 소프트웨어 설치·운영	21
8. 각급기관 PC통합보안시스템 운영	24
9. 사이버 보안 진단의 날 운영	28
10. MS Windows XP, Office 2003 지원 종료에 따른 컴퓨터 운영체제 및 오피스 프로그램 교체	39
11. 인천광역시교육청 웹메일시스템 운영	40
12. 웹사이트 접근 및 응용프로그램 차단	42
13. 학교홈페이지 통합 구축 사업	43
14. 웹 접근성(Web Accessibility) 이용 편의 제공	49
15. 보안서버 구축	51
16. 공공 I-PIN 서비스 도입	56
17. 웹취약점 점검 시스템 운영	60
III. 개인정보보호 업무 추진	64
1. 홈페이지 개인정보 유출 및 노출 방지 철저	64
2. 개인정보 노출 진단시스템 운영	65
3. 개인정보 침해사고 처분 기준	70
4. 개인정보업무 필수 이행사항	71
□ 업무별 문의처 안내	73

정보보안 및 개인정보보호 업무 추진 안내

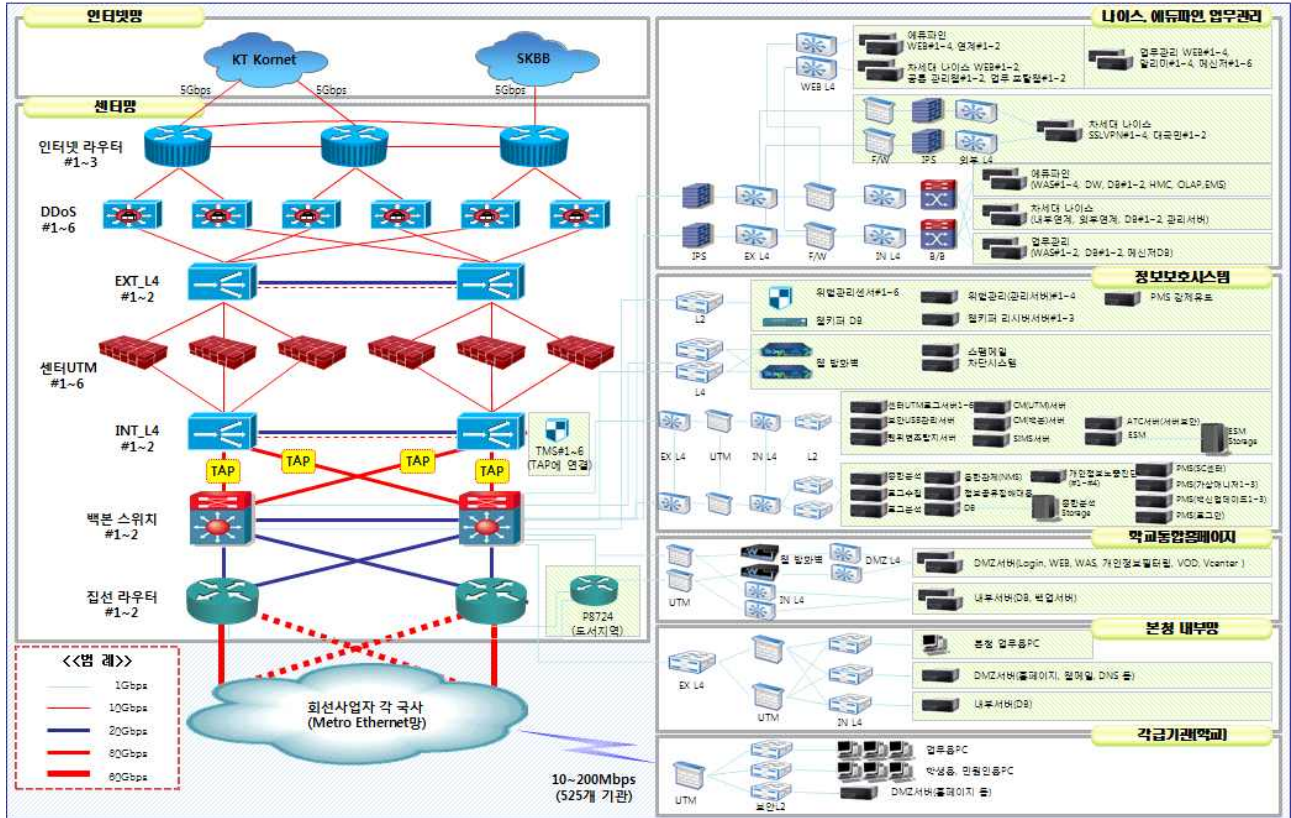
인천교육종합정보센터 정보보안시스템 현황

1. 운영 현황

구분	시스템	운영 범위	기능
PC 보안	백신관리	본청 및 산하기관 전체	백신 자동 업데이트 및 악성코드 차단
	패치관리	본청 및 산하기관 전체	PC보안 강화를 위한 Windows보안패치 및 백신 강제 설치
	보안USB	본청 및 사업소	보안USB관리 및 일반USB 차단
네트 워크	침입방지	본청 및 산하기관 전체	내부 네트워크로 유입되는 공격 탐지 및 대응
	침입차단	차세대나이스, 에듀파인	내부 네트워크로 유입되는 공격을 탐지
	종합분석	본청 및 산하기관 전체	모든 보안장비 이벤트를 종합 분석
	위협관리	본청 및 산하기관 전체	보안 위협정보 탐지
	DDoS차단	본청 및 산하기관 전체	DDoS 공격 차단
	통합보안장비	산하기관 전체	산하기관용 통합보안장비
	보안L2스위치	산하기관 전체	단말PC상 유해트래픽 차단
서버 보안	서버보안	차세대나이스, 에듀파인, 본청 및 교육지원청	서버 접근통제 및 보안 관리
웹/ 응용 보안	웹방화벽	본청 및 산하기관 전체	웹해킹 및 웹공격 탐지 및 차단
	웹메일	본청 및 산하기관 전체	기관용 및 개인용 보안 메일시스템
	스팸메일차단	본청 및 산하기관 전체	스팸메일 차단
	웹접속차단	본청 및 산하기관 전체	유해사이트 차단
	보안정보관리	본청 및 산하기관 전체	교육사이버안전센터에 보안로그 전달

2. 인천교육종합정보망 구성도

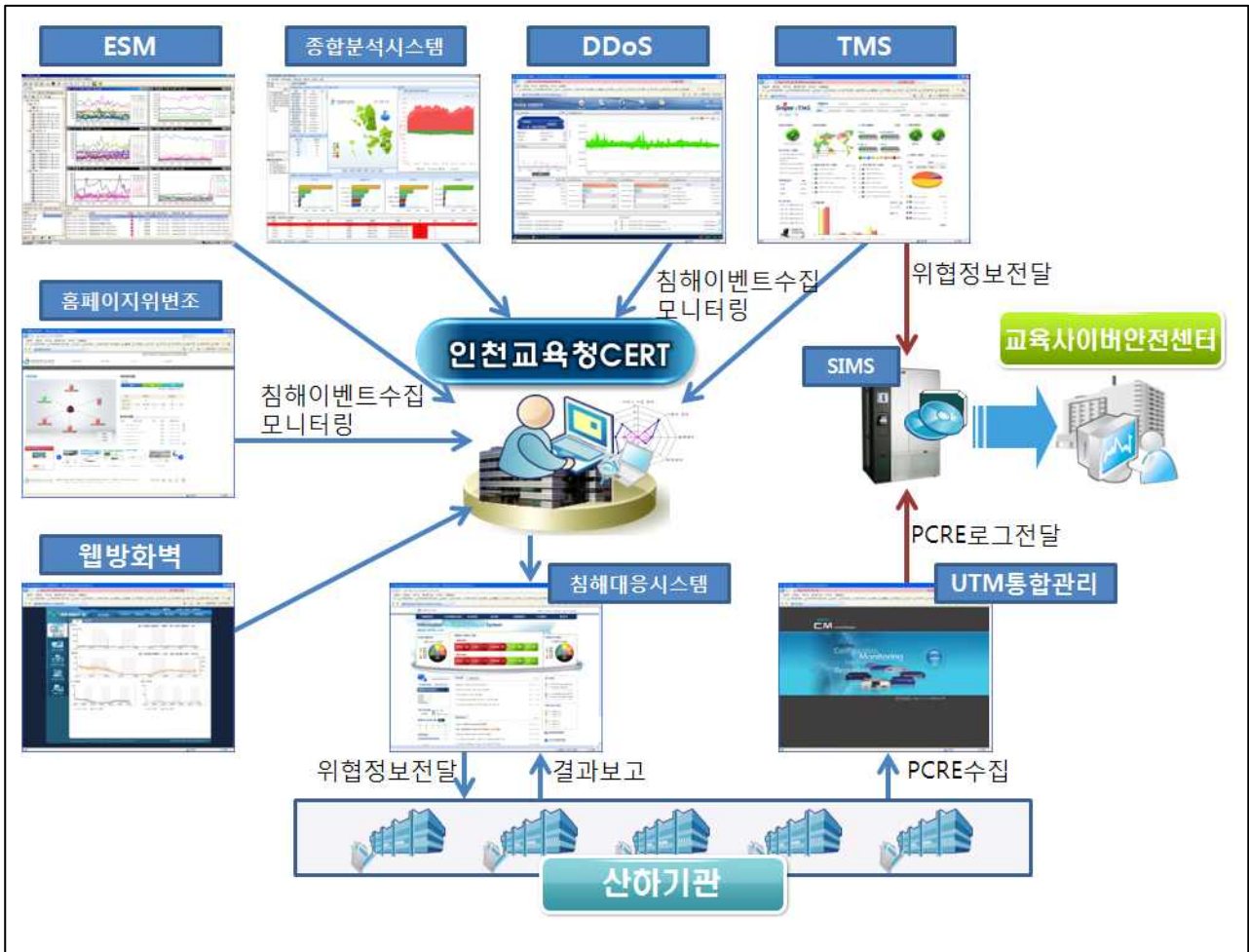
인천교육종합정보망 구성도



II 정보보안 추진 계획

1. 인천광역시교육청 정보보호 관리체계

가. 인천광역시교육청 보안관제 수행 개념도



나. 실시간 보안관제 분석 및 대응

- 종합분석시스템, 통합보안관제시스템 (ESM), 위협관리시스템 (TMS) 등을 통한 통합관제 실시
- 산하기관 통합보안장비 (UTM)에 PCRE탐지를 설정으로 실시간 보안관제 실시
- 보안정보관리시스템 (SIMS)을 통한 교육사이버안전센터와 연계

다. 정보공유 및 침해대응시스템(isac.ice.go.kr) 운영

- 각급기관 보안위협정보 및 침해사고 통보
- 홈페이지 개인정보노출진단내역 및 위변조내역 통보
- 사이버위기 예·경보 발령
- 최신보안뉴스, 보안권고문 등 보안정보 공유

2. 「인천광역시교육청 정보보안 기본지침」 개정 안내

가. 관련

- 「국가정보원법」, 「보안업무규정」(대통령령), 「정보 및 보안업무 기획·조정 규정」(대통령령), 「국가 사이버 안전 관리 규정」(대통령훈령), 「국가 정보보안 기본지침」, 「전자정부법」과 같은법 시행령, 「정보통신기반보호법」과 같은법 시행령, 「공공기록물 관리에 관한 법률 시행령」
- 「교육부 정보보안 기본지침」, 「교육부 사이버안전센터 운영규정」
- 「인천광역시교육청 보안업무 시행규정」

나. 개정 목적

- 정보보안 업무와 관련된 각종 법률, 규정에 따라 각급 기관이 수행하여야 할 기본 활동 규정을 그 목적으로 하되,
- 2013. 2. 26. 개정된 교육과학기술부 정보보안 기본 지침의 변경 사항을 반영하여, 교육(행정) 기관의 정보시스템 구축·운영 특성과 스마트교육 추진에 따른 학교 전역에 무선인터넷 관련 장비 설치 등을 지원하기 위함

다. 주요 개정 사항

- 1) 규정 완화에 관한 사항 : 스마트교육 추진에 따라, 학교 전역에 무선인터넷 관련 장비 설치·운영의 용이성과 인터넷 활용 교육, 인터넷전화 사용을 위한 정보보안 관련 규정 완화 반영
 - 지침 제3조(정의) : 인터넷서비스망, 업무전산망, 클라우드컴퓨팅, 클라우드서비스에 대한 정의 신설
 - 지침 제30조(인터넷 PC 보안관리) : **각급학교에 한하여 학교장 책임하에 교육 지원을 위한 상용 클라우드서비스 이용이 가능하도록 규정 추가**
 - 지침 제46조(무선랜 보안관리) : 각급학교의 경우 네트워크 이름(SSID, Service Set Identifier) 브로드캐스팅 중지, 추측이 어려운 복잡한 SSID 사용, DHCP 사용금지와 관련된 규정 적용 완화
 - 지침 제50조(무선인터넷 보안관리) : **각급학교는 교육 목적으로 무선인터넷을 사용하는 경우 기관 전역에 관련 장비 설치가 가능하도록 함**

- 다만, 무선망을 통한 업무망 정보시스템 접근을 정보보호시스템 등으로 차단하고, 교육감 또는 각급기관의 장이 정하는 무선랜 보안 대책을 강구하도록 함
- 지침 제52조(인터넷전화 보안관리) : 각급학교는 인터넷전화 시스템을 구축하거나 민간 서비스를 사용하고자 하는 경우 보안성 검토를 의뢰하지 않아도 됨

2) 정보보안 업무 권한·의무 규정 명확화 : 단설유치원, 초·중학교의 관리·감독 권한을 가지고 있는 교육지원청 교육장에게 산하 학교의 지도, 정보보안 감사에 관한 권한과 의무 명시

- 지침 제8조(지도방문), 제11조(정보보안 감사) : "교육감"을 "지도감독기관의 장"으로 조정

3) 정보보안담당자 교육 강화

- 지침 제12조(정보보안 교육) : 정보보안담당자는 의무적으로 연간 15시간 이상 정보보안 교육을 이수하도록 함

4) 국가 안보와 관련된 용역 사업에 대한 보안 규정 강화

- 지침 제57조(용역사업 보안관리) : 국가 안보(국방, 외교, 통일 등) 관련 용역 자료(연구, 자문 등)는 인터넷이 차단된 PC에 비밀번호를 부여하여 별도로 저장하거나 보안 USB에 저장하여 유출되지 않도록 조치하도록 함

5) 2011. 5월 이후 변경된 법률, 규정 등 반영

- 정부조직법 전부 개정에 따라 기존의 교육과학기술부를 교육부로 조정
- 「공공기관의 개인정보보호에 관한 법률」을 「개인정보보호법」으로 변경
- 2013. 1. 1. 변경 시행된 「인천광역시교육청 보안업무 시행규정」 반영
- 문맥 상 모호한 부분, 오·탈자 등 자구 수정

라. 개정된 지침 적용일 : 2013. 4. 1.부터

3. 정보공유 및 침해대응시스템 운영

가. 관련

- 「인천광역시교육청 정보보안 기본지침」

나. 목적

- 정보공유 및 침해대응시스템은 인천교육종합정보센터와 인천광역시교육청 산하 기관에서 운영 중인 모든 정보시스템의 사이버 침해사고 및 개인정보 노출 등에 대한 종합적인 예방과 효과적이고 신속한 대응을 위해 구축

다. 운영 안내

- 사용 대상 : 각급기관 정보보호 업무 담당자 누구나 가능
 - 신규사용자는 '신규사용자 등록(공인인증서 등록)' 후 별도의 승인과정 없이 로그인 가능함
 - 인사발령 등으로 소속기관 변경시 My Page에서 소속기관 수정 가능
- 기관 관리자 지정 : 각급기관 정보보안담당관 1인
 - 각급학교는 정보부장교사, 사업소는 정보보호 업무 담당자를 지정함
 - PC 운영현황, 홈페이지 운영현황 등 기관현황이 변경될 경우 My Page에서 수정 관리
 - 보안 위협정보 탐지·처리 및 사이버 침해사고 등을 운영·관리
- 기관별 보안위협정보 관리 및 사이버 침해사고 관리
 - 기관의 보안 위협 탐지 및 사이버 침해사고 발생시 기관 통보 및 조치 현황 정보 운영
 - 각급기관의 정보보안담당관은 기관에 보안 위협정보나 사이버 침해사고 발생시 즉시 조치하고 조치 결과를 입력해야 함
- 주요 정보보안 관련 정보 안내
 - 보안 권고문 안내, 보안 뉴스 링크, 정보보안 관련 참고자료실 운영 등 정보보안과 관련한 주요 정보 안내 및 관리

○ 기관별 주요 운영현황 관리

- 기관별 네트워크 회선 현황, 홈페이지 운영 현황, 개인정보 진단 현황, 웹 취약점 점검 현황 등 기관 내 정보보안 현황 안내 및 관리
- 기관의 운영현황 정보 변경시 즉시 수정 처리

○ 정보시스템 관리용(SSH, 원격데스크탑 등) 원격접속 요청

- 목적 : 기관 내 홈페이지 등 정보시스템을 원격지에서 네트워크로 접속, 정비하는 것은 원칙적 허용되지 않으나, 시스템 장애 등으로 긴급한 복구가 필요한 경우에만 요청·처리함
- 신청 : My Page에서 원격접속 요청 등록
- 주의사항
 - 원격접속 요청 전에 외부 유지보수업체로부터 '원격접속(보안 관련 룰셋) 요청서'를 징구할 것
 - 원격 접속 허용은 **최대 3일로 제한함**
 - ※ 원격접속요청은 장애복구에 필요한 작업시간에 한하여 최소한으로 요청하고, 월·분기단위의 정기유지보수 등은 직접 방문하여 처리
 - 원격 접속 요청 절차도



라. 2012년도 각급기관 보안 위협정보 현황

구분	유치원	초등학교	중학교	고등학교	사업소·기타	합 계
악성코드감염	1	56	23	37	13	130 (76%)
웹취약점 공격	0	21	4	9	7	41 (24%)
총 계	1 (0.5%)	77 (44.5%)	27 (16%)	46 (27%)	20 (12%)	171

- 악성코드 감염이 정보 보안 위협 현황중 76%를 차지함
- 악성코드 감염 방지를 위해서 '내 PC지키미' 시행, 바이러스 체이서 설치·점검 및 업데이트 시행 등을 준수

마. 2012년도 각급기관 사이버 침해사고 현황

구분	유치원	초등학교	중학교	고등학교	사업소·기타	합 계
악성코드감염	1	64	36	67	4	172 (96.6%)
해킹경유지악용	0	5	1	0	0	6 (3.4%)
총 계	1 (0.5%)	69 (39%)	37 (21%)	67 (37.5%)	4 (2%)	178

- 해킹경유지 악용 방지 등을 위해서 서버 OS를 최신 버전으로 패치 시행
- 「인천광역시교육청 정보보안 기본지침」 '제3절 전자정보 보안대책'을 참고하여 서버의 보안조치 반드시 시행
- 웹취약점 및 웹위변조 점검 시스템을 활용하여 주기적인 웹서비스 보호 활동 수행

4. 정보화 사업 보안성 검토 절차

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제68조 ~ 제71조
- 정보시스템 보안성 검토 가이드 안내(정보직업교육과-4159, 2012.03.13)

나. 목적

- 정보화사업 추진 시 자체 보안대책을 강구하여야 하며, 구축될 시스템에 대한 안전성을 확인하기 위하여 사업 계획단계에서 보안성 검토를 수행하여야 함

다. 보안성 검토 개요

- 보안성 검토(요청) 시기 : 정보화 사업 계획 단계(사업 공고 전)
- 보안성 검토 대상 사업 : 각급기관에서 실시하는 전체 정보화 사업
- 보안성 검토 처리 기간 : 접수 후 2주 이내(시교육청 자체 검토시)

라. 보안성 검토 처리

1) 보안성 검토 간소화

- 각급학교, 사업소 등은 소규모 기관으로 분류하여 자체 보안심사위원회 심사 생략
- 자체 보안심사위원회 심사는 생략하나, 상위기관으로 보안성 검토는 의뢰해야 함

2) 사업 규모 및 유형에 따른 보안성 검토 기관 분류

- 정보화사업의 예산 및 개인정보 DB화 규모와 사업유형의 구분 등에 따라 보안성 검토 기관 및 여부가 나뉨

가) 사업 규모 구분 : 예산 및 개인정보 DB화 규모에 따라 검토 기관 구분

보안성 검토 수행 기관	검토 대상 및 기준		
	예산	개인정보	유형
교육지원청, 시교육청	5억원 미만의 중소형 정보화사업	1만건 미만의 개인정보 DB화	정형화 유형
교육부	10억원 미만의 중형 정보화사업	100만건 미만의 개인정보 DB화	신규 유형
국가정보원	10억원 이상 대형 정보화사업	100만건 이상의 개인정보 DB화	업무망/인터넷망 분리 등 중요 현안사항

나) 사업 유형 구분 : '단순유형 정보화사업'과 '정형화된 정보화사업'으로 구분

사업 구분	내 용	보안성 검토 처리 여부
단순유형 정보화사업	<ul style="list-style-type: none"> • PC나 서버 등 단품 장비 도입 • 홈페이지 유지보수 등 	생략
정형화된 정보화사업	<ul style="list-style-type: none"> • 웹서비스 시스템 구축 • 무선랜 구축 등 14개 사업(아래 참조) 	수행

※ 정형화된 정보화 사업 유형

구분	정보화사업 유형	비 고
A 영역 관리	A-1 정보화사업 영역업체 보안관리	
B 주요 업무 인프라 구축	B-1 웹서비스 업무시스템 구축	
	B-2 내부망 전용 업무시스템 구축	
	B-3 외부기관 연계시스템 구축	
C 모바일 인프라 구축	C-1 무선랜 구축	
	C-2 모바일 오피스 구축	
D 응용 인프라 구축	D-1 원격 화상회의시스템 구축	
	D-2 CCTV시스템 구축	
	D-3 원격 백업시스템 구축	
	D-4 인터넷전화(VOIP) 구축	· 각급학교는 보안성검토 미 실시
	D-5 콜센터 시스템 구축	
E 시설 및 정보보안 인프라 구축	E-1 외부용 인터넷 PC 설치	
	E-2 네트워크 및 서버·PC장비 도입·교체	
	E-3 정보보호제품 도입	

- 보안성 검토 예시

가) A중학교에서 예산 900만원의 개인정보가 포함하지 않는 무선네트워크 구축 사업을 시행하는 경우

⇒ 예산 5억원 미만, 개인정보 1만건 미만, 정형화유형 사업이므로, 해당 교육지원청에서 보안성 검토 처리

- ① 자체 보안대책을 수립한 후 "보안성 검토 가이드"를 참고하여 해당 교육지원청으로 보안성 검토를 의뢰
- ② 해당 교육지원청에서 보안성 검토 실시 후 A중학교에 결과 통보
- ③ A중학교에서는 보안성 검토 결과를 반영하여 정보화사업 수행

나) B도서관에서 예산 2,000만원의 개인정보가 2만건의 홈페이지를 신규 구축하는 사업을 시행하는 경우

⇒ 예산 5억원 미만, 개인정보가 1만건 이상, 두 개의 조건중 하나만 해당되는 정보화유형 사업이므로 교육부로 보안성 검토 처리

① 자체 보안대책을 수립한 후 본청(정보지원과)으로 보안성 검토 요청

② 본청에서는 해당 건을 교육부로 이첩

③ 교육부에서 보안성 검토 실시 결과 통보시 B도서관에 결과 이첩 통보

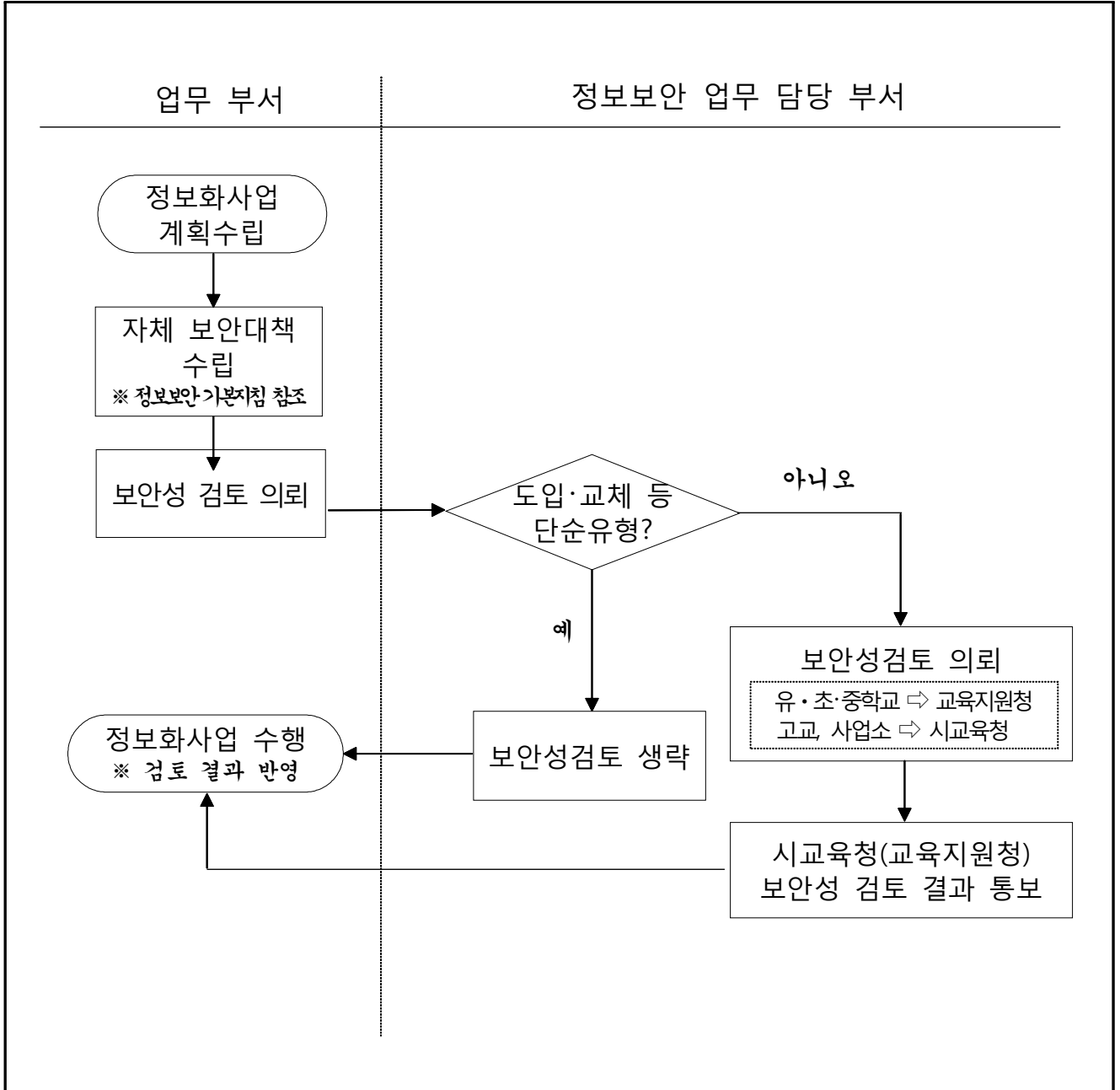
④ B도서관에서는 보안성 검토 결과를 반영하여 정보화사업 수행

마. 제출자료

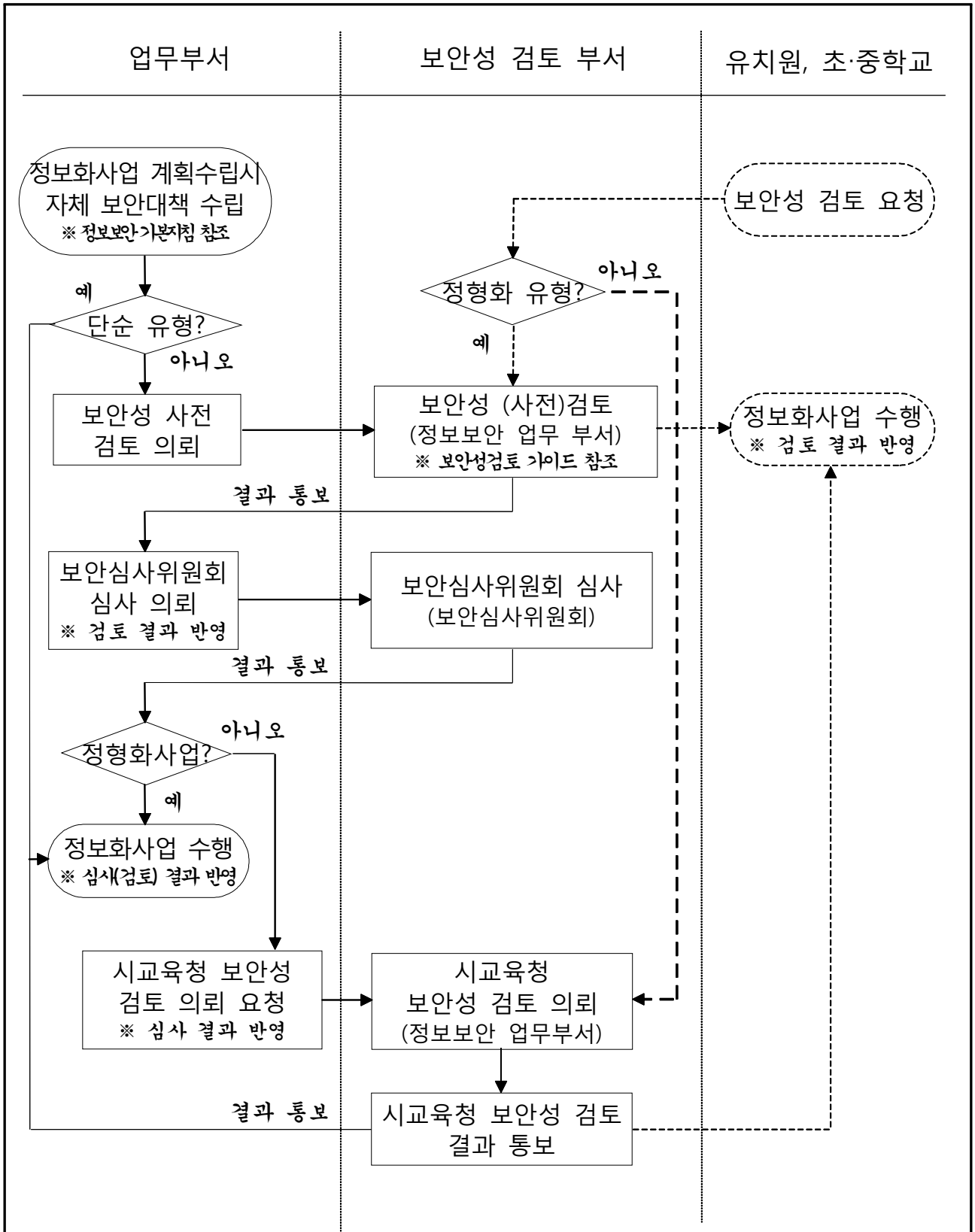
- 사업계획서(사업목적 및 추진계획 포함)
- 기술제안요청서(RFP)
- 정보통신망 구성도(IP주소 체계 포함)
- 자체 보안대책 강구 사항
 - 보안관리 수행체계(조직, 인원)등 관리적 보안 대책
 - 정보시스템 설치장소에 대한 보안관리 방안 등 물리적 보안대책
 - 국가용 보안시스템 및 국정원장이 개발하거나 안정성을 검증한 암호모듈, 정보보호시스템 도입 운용 계획
 - 국가기관 간 망 연동 시 당해 기관 간 보안관리 협의사항
 - 서버, 휴대용 저장매체, 네트워크 등 정보통신망의 요소별 기술적 보안대책
 - 재난복구계획 또는 상시 운용 계획

□ 기관별 보안성 검토 상세 절차

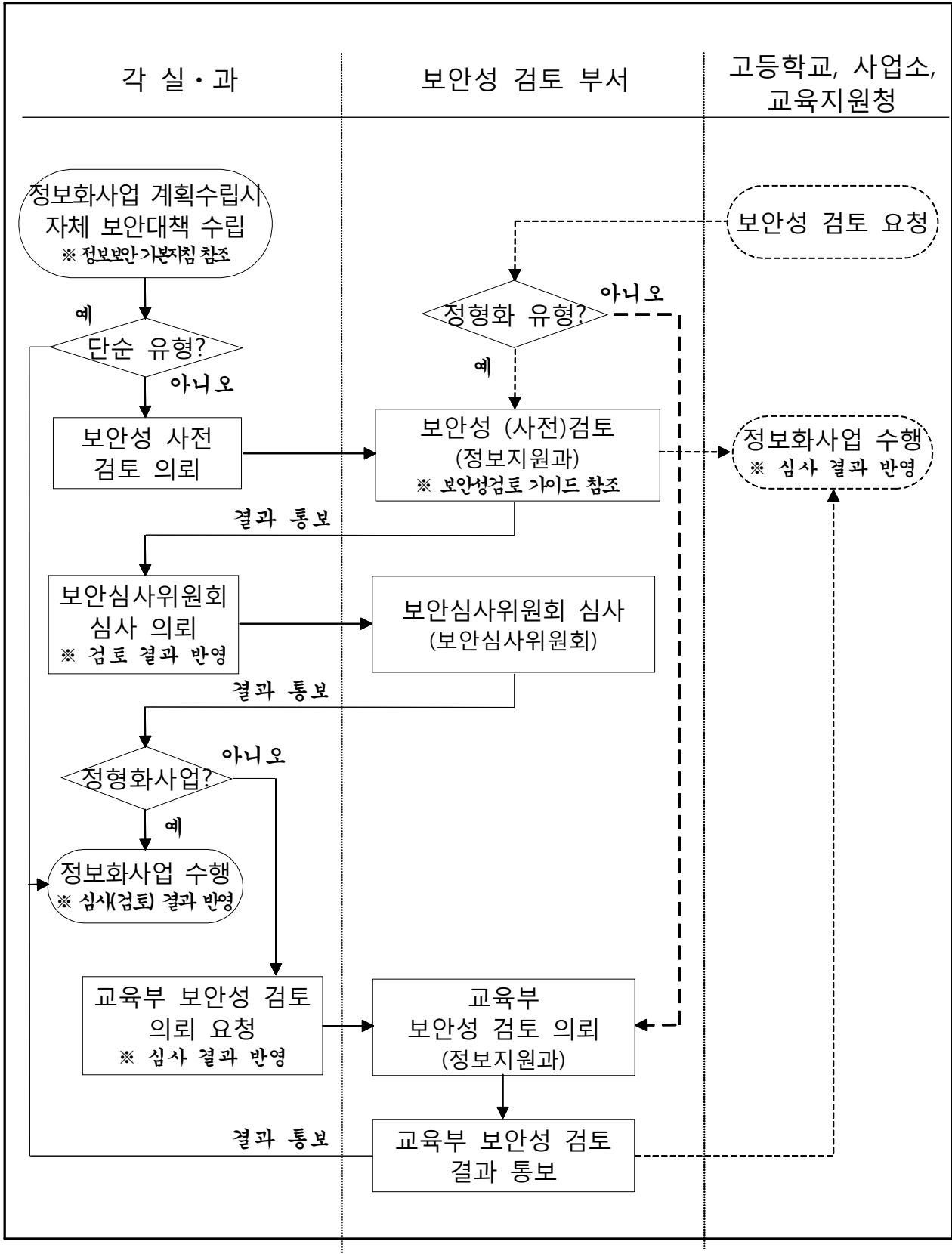
◆ 각급학교, 사업소



◆ 교육지원청



• 시교육청



5. 무선랜 보안관리

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제46조(무선랜 보안관리)
- 정보화사업 보안성 검토 가이드 안내(정보직업교육과-4159, 2012.03.13)

나. 주요 내용

- 무선랜은 기본적으로 통신거리의 한계가 분명치 않고, 무선랜을 이용한 해킹사고가 발생할 경우 원인규명 어려움
- 무선랜(와이파이 등) 시스템을 구축시에는 자체 보안대책을 수립하여 관련 사업 계획 단계에서 반드시 보안성 검토 상위기관(교육지원청 또는 시교육청)으로 보안성 검토 의뢰
- 국가·공공기관의 업무영역에서 무선랜을 운용하는 것은 원칙적으로 불가
 - 기관 네트워크와 연동하여 사용해야만 할 경우는 아래 정보의 접근 통제 및 관리사항을 준수
 - 상용 ISP에서 제공하는 무선랜 서비스를 이용하여 민간인 등 외부인의 인터넷 접속용으로만 사용토록 권고
 - 각급학교에서 스마트교육을 목적으로 추진하는 무선랜 구축 사업은 스마트교육사업부서(정보직업교육과 학교정보지원팀)와 사전 협의 바람

다. 보안성 검토 의뢰시 반드시 포함해야 할 보안대책

- 네트워크 이름(SSID, Service Set Identifier) 브로드캐스팅 중지(단, 각급학교는 제외)
- 추측이 어려운 SSID 사용(단, 각급학교는 제외)
- WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화
- 무선랜 장비 접속시 MAC 주소 및 IP 필터링 설정
- 무선랜 장비의 DHCP 사용 금지(단, 각급학교는 제외)
- 무랜 AP(Access Point)연결 시 사용자 인증은 RADIUS(Remote Authentication Dial-In User Service) 인증 사용

- 무선망을 통한 업무망 정보시스템 접근을 정보보호시스템 등으로 차단하는 보안대책
- 무선단말기·중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책

라. 구축 시 고려사항

- 네트워크 담당자는 기관 내에서 설치된 무선랜 장비의 운영현황을 철저히 파악하여 관리
- 무선랜 장비의 보호를 위해 전파가 건물 내에 한정되도록 전파 출력을 조정하고, 창가나 외벽 쪽이 아닌 건물 중심부에 보이지 않게 설치
- 무선랜 장비의 기본 관리계정 및 패스워드는 반드시 재설정
- 무선랜은 스니핑, MAC 스푸핑, WEP 크랙, 서비스 거부공격, 세션 가로채기 공격 등에 취약할 수 있으므로 이에 대한 대응책 마련

6. 정보화사업 용역업체 보안관리 강화대책

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제57조(용역사업 보안관리)
- 「지방자치단체를 당사자로 하는 계약에 관한 법률 시행령」 제92조(부정당업자의 입찰 참가자격 제한) 제1항 제19호

나. 배경

- 각급기관 정보화사업 과정에서 용역업체의 사업관련 자료 무단유출·보관, 정보시스템 유지보수업체의 보안관리 부실로 개인정보유출 및 정보보안사고 발생

다. 주요 사고 사례

- 2009. 6월 OO도내 25개 공공기관 전산망 유지보수업체 A社 전직 직원은 전산망 구성도, 접속 ID·비밀번호 등을 USB에 저장, 무단 반출
- 2009. 5월 보안패치관리시스템 업체 C社 직원 PC가 해킹되어 OO청 등 3개 기관 보안패치관리시스템 접속 ID·비밀번호가 유출
- 2010. 5월 정보시스템 유지보수 업체 D社는 기관의 승인없이 무단으로 서버에 불법 모듈 설치하였고, E社는 관리자 PC에서 서버의 정보를 중간에서 파싱 방식으로 불법 이용
- 2011. 4월 OO은행 용역업체인 F社의 직원 노트북 PC에서 삭제 명령 실행으로 전산망 마비 및 거래내역 일부 유실

라. 보안관리 강화 대책

- 정보화사업 용역업체 점검 및 관리감독 강화
 - 용역업체가 정보누출 적발 시 부정당업자로 등록, 입찰 참가자격 제한 등 제재 조치 가능
 - 시스템을 통해 유지보수업체가 정보자원에 접근을 차단하는 것이 원칙이나, 허용할 경우에는 접근을 최소화
 - 업체의 작업내역을 상시 점검, 비정상적 행위 감독
 - 용역 참여인원에 대한 변동사항을 재확인하고 보안서약서 징구, 보안사고 유발

- 시 과급영향 등 보안교육을 실시, 경각심 제고
 - 업체에 제공한 전산망 구성도·IP주소 현황 등 비공개 자료 관리실태 및 인터넷 연결 PC에 개발·유지보수 관련자료 보관여부 등 점검
 - 기관 전산망 접속권한 계정 부여현황 및 작업이력 확인, 비인가 노트북 PC·USB 등에 자료 무단 보관 및 반출·입 여부 점검
 - 서버 작업은 반드시 기관 담당자 입회·감독 하에 실시, 작업 완료 후 작업이력을 점검하여 보안책임자에게 승인을 받음
- 용역 업체 대표 명의 보안서약서 징구
- 계약서에 보안준수사항, 자료 반환 및 위반 시 손해배상 책임 등 보안관련 특약조항 명시
 - 사업 착수 시 용역업체 자체 보안관리 및 직원 관리감독 강화를 독려하고 보안의 중요성 인식제고를 위해 업체대표 명의 보안서약서 징구
 - 사업완료시 용역관련 제반자료 전량 회수, 저장매체 내 자료 삭제 및 사업산출물 복사본 등을 보관하지 않는다는 대표명의 확약서 징구
- 정보시스템의 원격 유지보수 시 보안강화
- 정보시스템을 원격지에서 네트워크로 접속, 정비하는 것은 원칙적 금지
 - 정보시스템 장애 등으로 긴급한 복구가 필요한 경우 반드시 업체로부터 "원격 접속 요청서"를 징구하고, **정보공유 및 침해대응시스템**(<http://isac.ice.go.kr>)에 원격접속 요청(자세한 내용은 9쪽 '정보시스템 관리용 원격접속 요청' 참고)
- 정보화 사업 추진 시 보안성 검토시에는 교재 11쪽 "4. 정보화 사업 보안성 검토 절차" 참조

7. 정보보호 소프트웨어 설치·운영

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제44조(전자정보 저장매체 불용처리)
- 「개인정보보호법」 제29조(안전조치의무)
- 정보보호를 위한 소프트웨어 배포 안내(정보직업교육과-1808, 2010. 9. 30.)

나. 목적

- 주민번호 등 다양한 개인정보가 포함된 전자문서의 검색·삭제·암호화를 통해 개인정보의 안전성을 확보하고, PC 저장자료를 완전 삭제하여 폐기·양여 시 중요정보의 외부 유출을 방지하고자 함

다. 배포 소프트웨어

소프트웨어명	주요 기능	비고
HDD 완전삭제 프로그램 (BlackMagic v2.0)	<ul style="list-style-type: none"> • 파일 및 폴더 삭제 • 파일 검색 및 검색파일 선택 삭제 • 미사용 영역 청소, 디스크 청소 • 파티션별, 디스크 병렬 삭제 등 • 보조기억매체(FDD, USB 메모리) 삭제 지원 	국정원 CC인증 제품
PC 개인정보 검색 프로그램 (I-Safer v2.0)	<ul style="list-style-type: none"> • 주민번호 등 8가지 종류 개인정보 검색 • 개인정보 파일 검색, 암호화, 숨김 기능 • 예약 검색, 특정문자열 검색 등 • 검색 이력, 통계 등 관리정보 제공 	

라. 소프트웨어 설치·사용

- 설치대상 : 교육청 산하 전 기관 업무용 PC
 - ※ 학생용 PC도 설치 사용 가능
- 설치환경 : 윈도우 계열(Windows XP, Vista, 7 등) PC 및 서버
- 설치·사용방법 : ISAC [보안정보-참고자료실] 36번에 설치방법 및 설치파일 탑재(CD 부팅용 BlackMagic-SA는 제외)

○ 유의사항

- 해당 프로그램으로 파일/폴더/디스크 삭제 시 복구 불가
- HDD 완전삭제 프로그램 CD(BlackMagic-SA) 부팅 시 인증 확인 필요
(ID : icecert / Password : iceBM2010)

마. 행정사항

- PC 신규·재설치 시에도 빠짐없이 설치(윈도우 계열 서버도 반드시 설치)
- PC 폐기·양여 시 HDD 완전삭제 프로그램을 사용하여 반드시 HDD 삭제
 - ※ HDD 재사용 가능
- 기관 모든 업무용 PC에 개인정보 검색프로그램을 반드시 설치하여 "사이버보안 진단의 날"에 필수 수행
 - 월 1회 이상 개인정보 검색, 삭제 또는 암호화 조치 수행(주민등록번호 항목은 필수 검색)
 - ※ 검색 경로에 모든 폴더 설정 후 검색 수행(C:\, D:\ 등)
 - ※ 설치 시 사용자명 정확히 입력
 - 설치 후 사용자명 변경은 [환경설정-일반-관리서버]에서 변경
 - ※ 보안감사 및 현장 점검 시 프로그램 설치·사용현황 확인 예정
- PC를 제외한 정보시스템(웹서버 등) 디스크는 본청 정보지원과로 파기 요청
 - 인편으로 <별첨>파기요청서와 파기 디스크 인계
 - ※ 본청 자기소자 장비(디가우저)로 디스크 파기 시 재사용 불가

※ 개인정보 보호법 시행(2011.9.30)
 주민등록번호 등 고유식별정보 안전성 확보 조치를 하지 않거나
 목적달성 및 보유기간이 경과한 개인정보를 파기하지 않은 경우
 ⇒ 3천만원 이하의 과태료 부과

<별첨>

디스크 파기 요청서

작성일 : 20년 월 일

대상장비	시리얼 번호	용도	수량	비고

요청자		작업자	
성명		성명	
소속		소속	인천광역시교육청
직책		직책	
연락처		연락처	
서명		서명	

※ 작성 요령

- 대상장비 : 해당 디스크가 장착되어 있던 시스템(서버)명 기재 ex) Sun Fire 3800
- 시리얼번호 : 디스크 시리얼 번호 기재
- 용도 : 해당 디스크 용도 기재 예) 웹서버, DB서버, 파일서버 등
- 수량 : 디스크 수량

8. 각급기관 PC통합보안시스템 운영


가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제29조(PC 등 단말기 보안관리), 제40조(악성코드 방지대책)
- 각급 기관 PC통합보안시스템 교체에 따른 프로그램 배포 안내 (정보직업교육과-855, 2011. 1. 20.)
- PC통합보안시스템 바이러스 백신 업그레이드 알림 (정보직업교육과-11685, 2011. 6. 27.)

나. PC통합보안시스템

- 패치관리시스템 : SC(Security Center) Agent
- 바이러스 백신 : 바이러스채이서(Virus Chaser) 8.0

다. SC Agent 설치

- PC
 - SC Agent 강제설치유도 페이지를 통한 설치
 - 정보공유 및 침해대응 시스템(<http://isac.ice.go.kr>)의 왼쪽 링크 중 를 클릭하여 설치
- 서버 : SC Agent를 설치하지 않음

라. Virus Chaser 8.0 설치

- PC
 - SC Agent에 의해 자동 배포 및 설치되나, 수동 설치하고자 하는 경우
 - 정보공유 및 침해대응 시스템(<http://isac.ice.go.kr>) - [보안정보] - [참고자료실]의 42번 게시물 "[PMS, 백신] SC Agent & Virus Chaser 8.0 설치 파일"을 다운로드
 - 압축파일 내의 "VC80Setup3_20111206(일반용).exe" 실행

○ 서버

- 서버에는 SC Agent를 설치하지 않으므로, Virus Chaser 8.0을 수동설치
- 다른 백신이 이미 설치되어 있는 경우, 삭제하고 재부팅 후 Virus Chaser 8.0(서버용) 설치
 - 정보공유 및 침해대응시스템(<http://isac.ice.go.kr>)-[보안정보]-[참고자료실]의 42번 게시물 "[PMS, 백신] SC Agent & Virus Chaser 8.0 설치 파일"을 다운로드
 - 압축파일 내의 "VC80Setup_20110713d(서버용).exe" 실행

○ 기술지원

- SC Agent, Virus Chaser 8.0 관련 : ☎ 420-8428
- 바이러스 감염 의심 시 : Virus Chaser 바이러스 대응팀 ☎ 070-7308-1004
- 정보공유 및 침해대응시스템(ISAC) PC보안센터 문의 게시판

○ 주의사항 : V3 Lite, 알약 등 타 백신 설치 금지


- Virus Chaser 8.0이 설치되어 있는 PC에 V3 Lite, 알약 등 타 백신을 설치하는 경우, 이중 백신 간에 서로 충돌이 발생하여 시스템이 다운되거나, 인터넷이 차단되는 현상이 발생할 수 있으므로, 타 백신은 가급적 설치 지양
- 이미 설치되어 이상 증상이 나타나는 PC의 경우 "안전모드"로 부팅하여 타 백신 삭제 후 재부팅

마. Web Security Center

○ 제공 기능

- SC Agent 및 Virus Chaser 설치 현황
- 보안 패치 및 백신 엔진 업데이트 내역 관리

○ 접속 방법

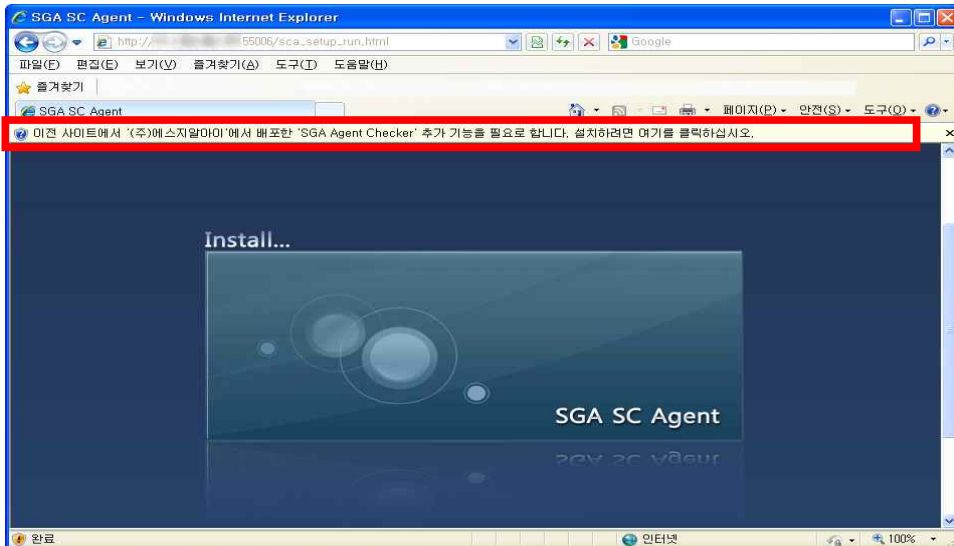
- 정보공유 및 침해대응 시스템(<http://isac.ice.go.kr>)의 왼쪽 링크 중 를 클릭하여 접속하거나 URL(<http://125.133.128.218:55008>)을 입력하여 접속

- SGA SC 서버 주소 : 125.133.128.218
- 서버 포트 : 55001

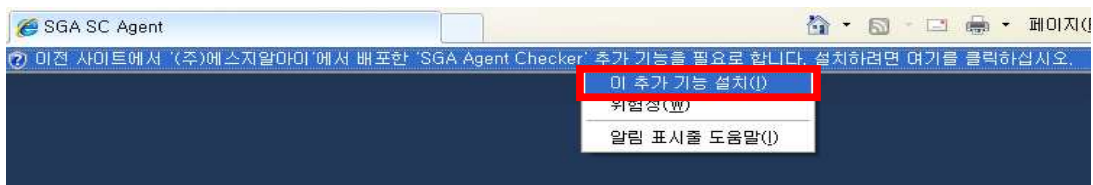


바. SC Agent 강제설치유도

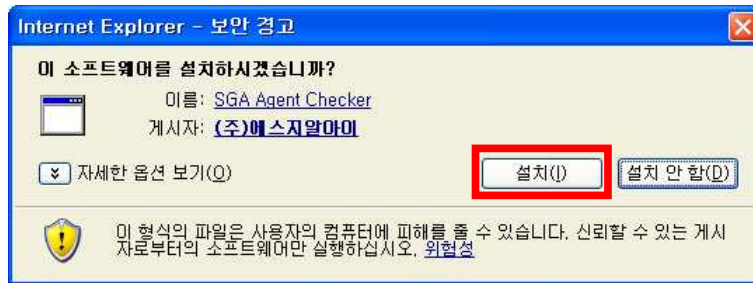
- SC Agent를 강제적으로 설치하도록 하는 기능
- 강제설치유도를 통한 SC Agent 설치
 - SC Agent가 설치되어 있지 않은 PC에서 웹사이트에 접속을 시도하면 SC Agent 설치유도 화면이 나타나게 됨



- "SGA Agent Checker"(ActiveX) 설치를 위해 "이 추가 기능 설치(I)" 클릭



- "SGA Agent Checker"(ActiveX) 설치



- ActiveX 설치 완료 후 "SC Agent" 설치를 위하여 아래 창에서 "설치하기" 버튼 클릭



9. 사이버 보안 진단의 날 운영

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제13조(사이버보안진단의 날)

나. 시행일 및 범위

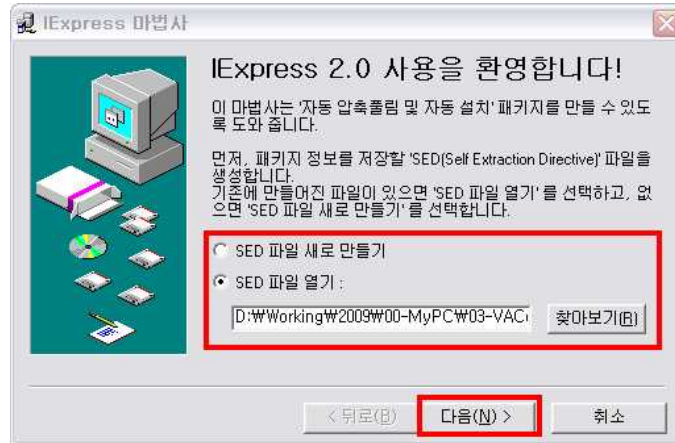
- 시행일 : 매월 세 번째 수요일에 시행
- 시행범위
 - 업무용PC : 교직원이 사용하는 전체 PC 및 노트북(학교회계직원, 공익요원 등 포함)
 - 교육용PC : 전산실습실 및 교실에서 사용하는 모든 PC 및 노트북
- 시행방법 : "내PC지키미"를 실행하여 PC 취약점을 진단하고, 취약으로 나온 항목을 조치하여 안전으로 전환

다. 진단 프로그램

- 프로그램 다운로드
 - 정보공유 및 침해대응시스템(<http://isac.ice.go.kr>)의 [보안정보]-[공개자료실]-3번 게시물 "내PC지키미 2.10.01.031 (Windows 7 호환)"
- 각 기관별로 내PC지키미 진단 프로그램 배포파일 생성 (배포파일 생성은 Windows XP PC에서 작업)
 - 1) "1.내PC지키미 배포파일 생성도구" 폴더를 더블클릭
 - 2) MyPCInspector 폴더의 setup 파일을 수정

```
[AXCLEAN]
ALLOWIP=127.0.0.1;localhost
[INSTALL]
HNC_ON=0
VERSION=2.10.01.031
SERVERIP=PC진단결과확인시스템이 설치된 PC의 IP를 입력
SERVERPORT=60000
HNC_SERVERPORT=60001
```

- 3) "배포파일생성도구" 폴더를 열어 iexpress.exe 실행
- 4) [SED 파일 열기]를 선택하여 배포된 SED 파일을(상위폴더에 위치) 선택 후, [다음] 클릭 (예: 내PC지키미프로그램(2.10.01.031).SED)



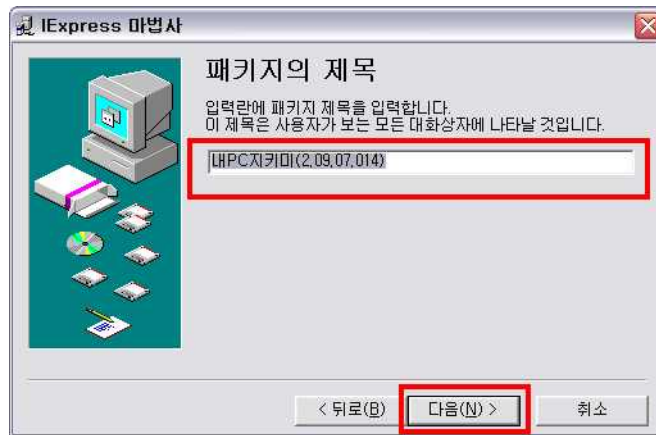
- 5) [SED 파일 수정하기]를 선택 후, [다음] 클릭



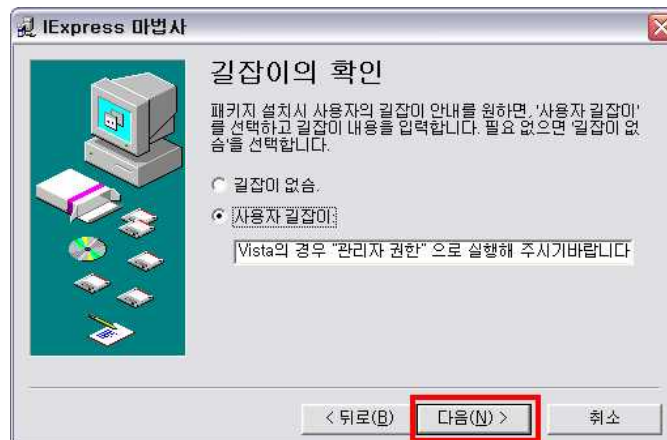
- 6) [파일의 압축을 풀고 설치 실행하기]를 선택 후, [다음] 클릭



7) 원하는 패키지의 제목[내PC지키미(2.10.01.031)]을 입력하고, [다음] 클릭



8) 사용자에게 공지하고 싶은 내용을 입력하고, [다음] 클릭
(예 : Windows Vista, Windows 7의 경우 "관리자 권한" 으로 실행해 주시기 바랍니다. 설치를 계속 진행하시겠습니까?)



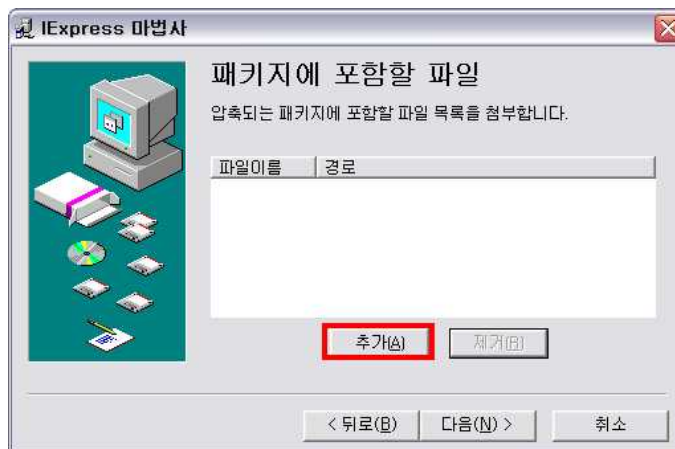
9) [다음] 클릭



- 10) 처음으로 배포파일을 생성하는 경우, 경로를 재설정해주어야 하므로 모든 파일을 선택(첫 파일을 선택 후, [Shift]를 누르고 맨 마지막 파일을 선택)하여 [제거] 선택



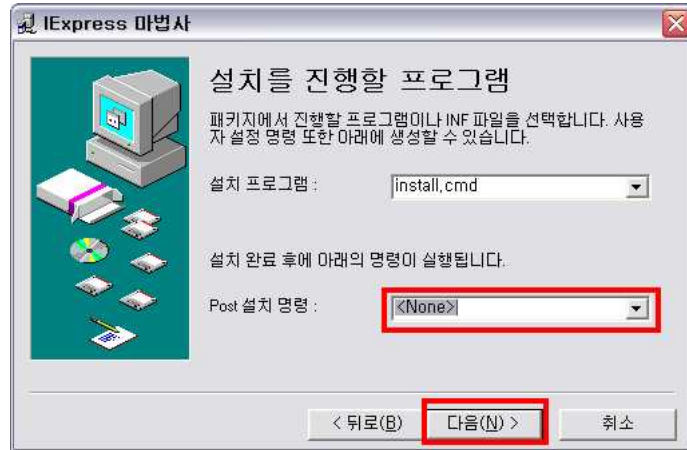
- 11) [추가]를 선택하여 MyPCInspector 폴더 안의 모든 파일을 선택



- 12) [다음] 클릭



13) 설치를 진행할 프로그램은 따로 선택하지 않고, [다음] 클릭



14) [기본값(권장)]을 선택 후, [다음] 클릭

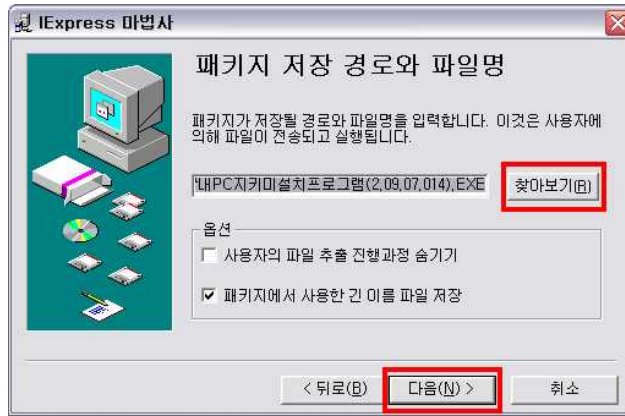


15) [메시지 없음]을 선택 후, [다음] 클릭



16) [찾아보기]를 선택하여 설치파일의 생성 저장위치 및 파일이름을 입력하고, [다음] 클릭

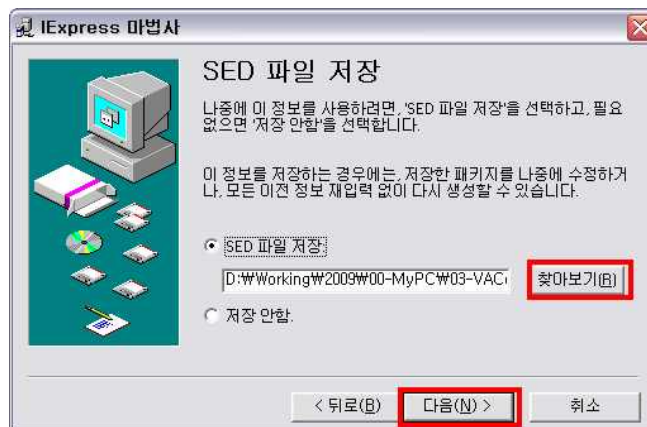
<주의!!!> 설치프로그램이 저장되는 폴더의 위치를 반드시 기억해야 함



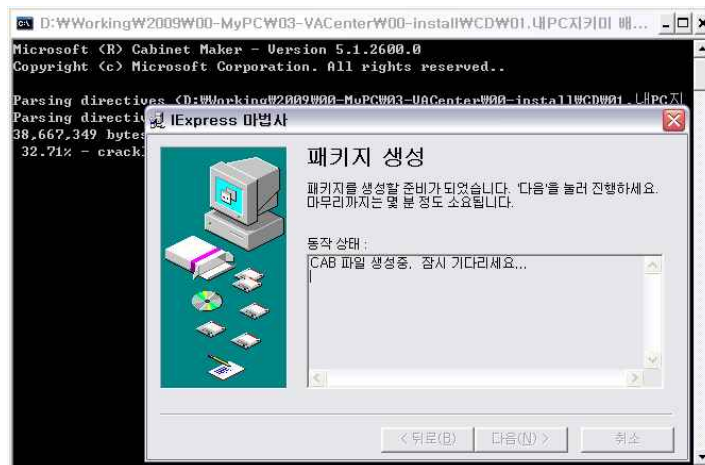
17) [재시작 안함]을 선택 후, [다음] 클릭



18) SED 파일의 이름을 변경하고 싶은 경우, [찾아보기]를 선택하여 SED 파일의 저장위치 및 파일이름을 입력하고, [다음] 클릭



19) [다음] 클릭



20) 설치파일 생성완료. [마침] 클릭



21) 16)번에서 지정한 폴더위치에 "내PC지키미설치프로그램"이 생성되었는지 확인

22) 생성된 프로그램을 각 개별PC에 배포하여 설치

○ PC진단결과통계(VACenter) 프로그램

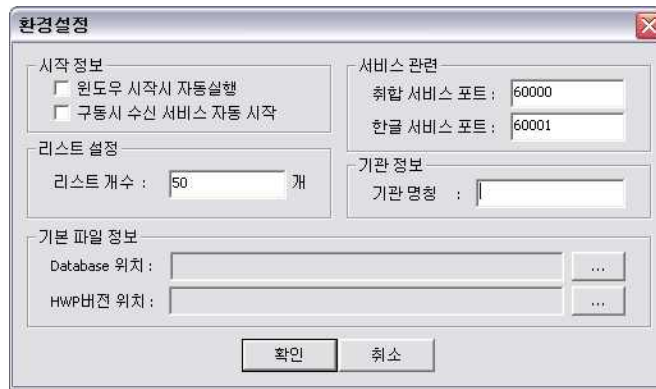
1) 내PC지키미 점검결과 취합을 위한 PC 또는 서버를 지정

※ 지정한 취합PC의 IP는 위에서 입력한 setup 파일의 SERVERIP와 동일해야 함

2) "4.PC진단결과 확인시스템"폴더 내 "VACenter"폴더를 원하는 위치에 복사

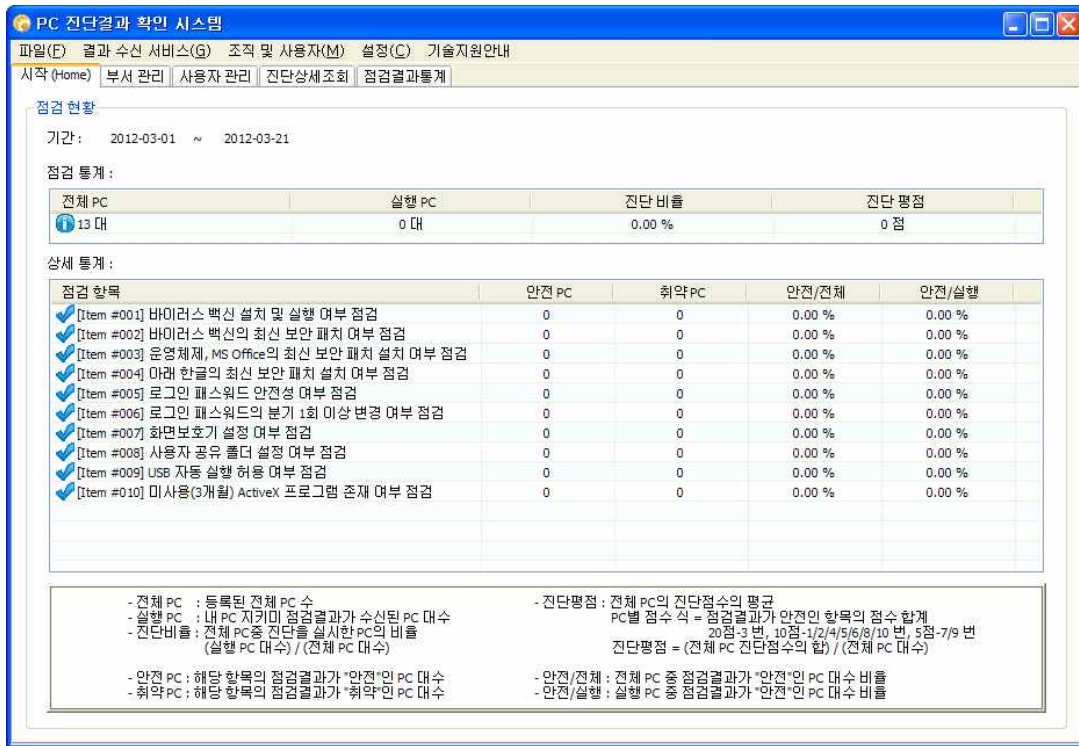
3) "VACetner"폴더 내에 있는 "VACenter.exe"를 실행

4) 환경설정 : PC진단확인시스템을 처음 실행하면 아래와 같은 환경설정 화면이 표시됨



- 윈도우 시작시 자동실행 : 선택하면 다음 윈도우 시작시마다 자동 실행
- 구동시 수신 서비스 자동 시작 : 선택하면 프로그램 실행 시마다 수신 서비스가 자동 실행
- 리스트 개수 : 진단결과 상세조회 시 리스트의 개수 (10~1024의 이내의 값)
- 취합 서비스 포트 : 60000(변경하지 않음)
- 한글 서비스 포트 : 60001(변경하지 않음)
- 기관명칭 : 기관의 명칭을 입력
- Database 위치 : 진단결과를 저장할 파일의 위치를 지정 (해당 폴더에 VACenter.mdb 가 생성됨)
- HWP버전 위치 : VACenter 폴더에 위치한 HWPVersion.txt을 선택

5) 내용을 입력하고, [확인]을 선택하면 다음과 같은 화면이 표시됨

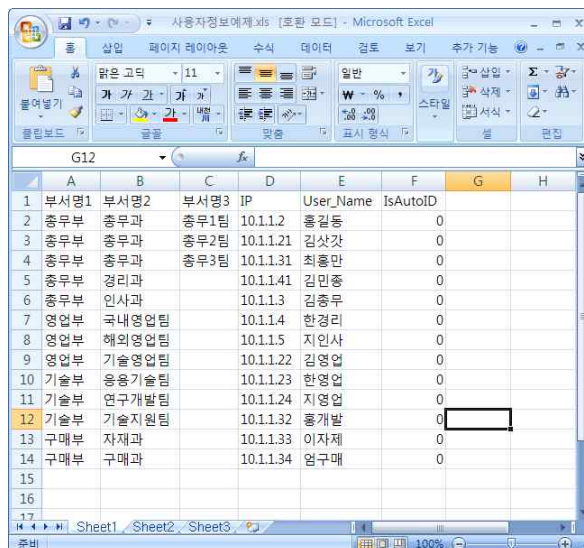


6) "결과 수신 서비스" 시작 여부 확인 : "수신 시작" 메뉴가 회색으로 되어 있어야 내PC지킴이 점검 결과를 받을 수 있는 상태임

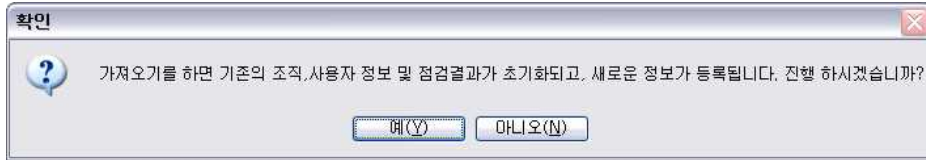
7) 부서 관리, 사용자 관리

가) 엑셀 파일을 작성하여 부서 및 사용자 등록

- "4.PC진단결과 확인시스템"폴더의 "부서 및 사용자 등록예제파일" 폴더의 "사용자정보예제.xls" 오픈
- 부서명, IP, 사용자 이름, IsAutoID 순으로 엑셀파일 작성

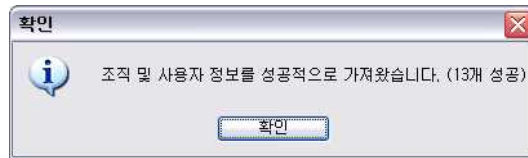


- PC진단결과 확인시스템의 [조직 및 사용자-가져오기]를 선택

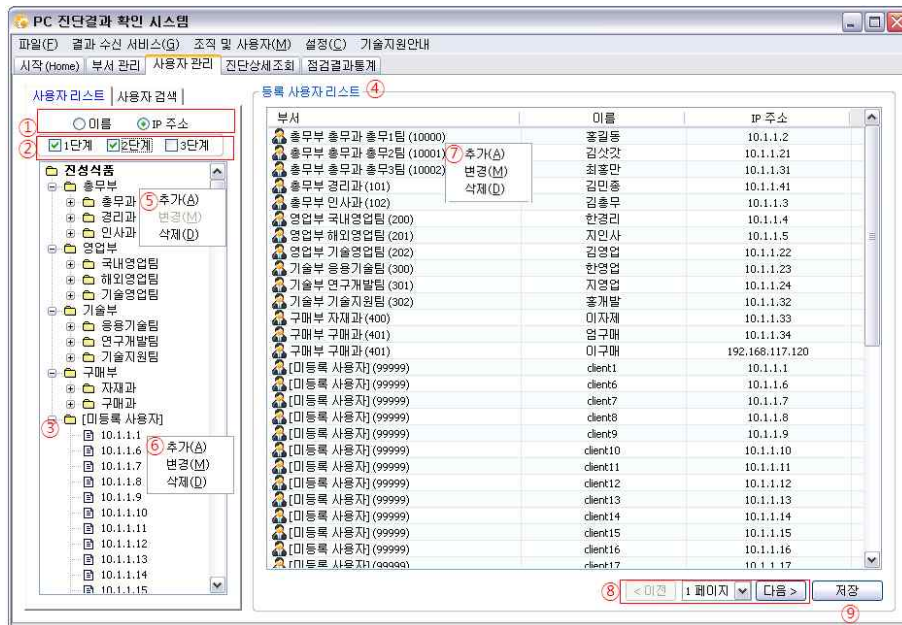


※ 주의!! : 가져오기를 실행하면 이전의 사용자 정보 및 점검결과가 초기화됨

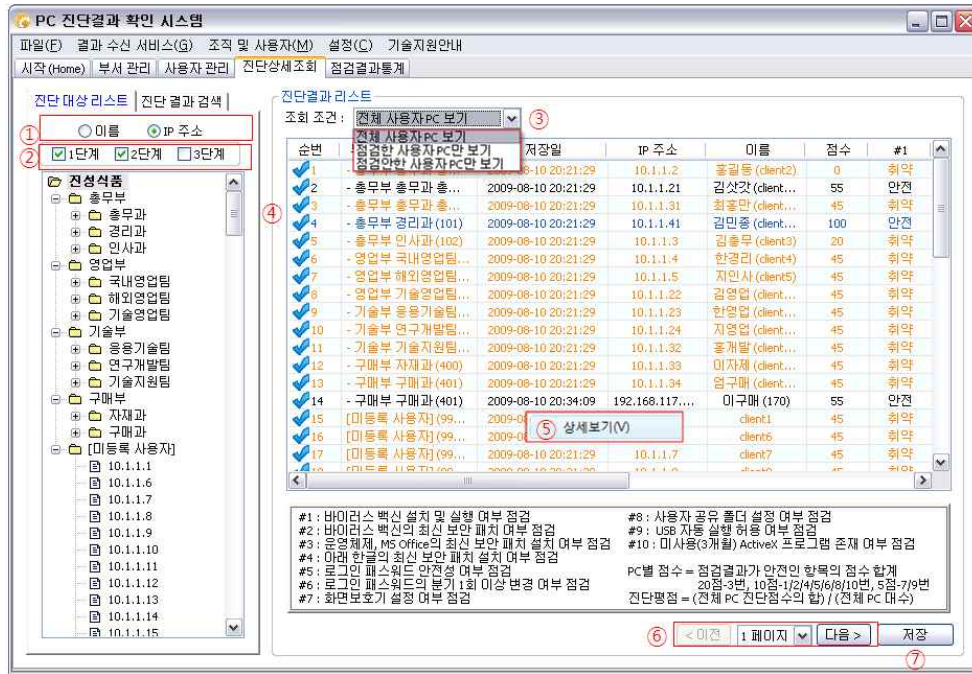
- 조직 및 사용자 엑셀파일을 선택(예: 사용자정보예제.xls)
- 가져오기 결과가 표시됨



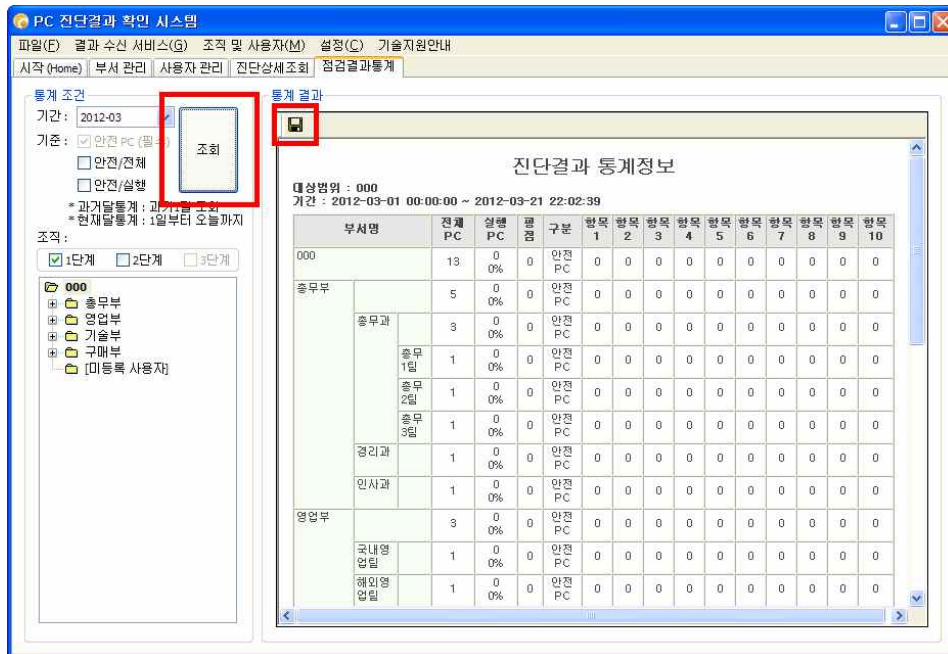
나) 마우스 오른쪽 버튼을 눌러서 부서정보 변경 및 사용자정보 변경



8) 진단상세조회 : 각 PC사용자의 점검결과 조회



9) 점검결과통계 : [조회] 버튼을 눌러 점검결과를 확인한 뒤, 디스크 모양의 아이콘을 클릭하여 점검결과를 저장 및 출력하여 자체보관



10. MS Windows XP, Office 2003 지원 종료에 따른 컴퓨터 운영체제 및 오피스 프로그램 교체

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제29조(PC 등 단말기 보안관리)

나. 목적

- MS에서 Windows XP 및 Office 2003 보안패치 제공을 2014. 4. 8.부터 중단함에 따라 해당 제품을 그대로 사용할 경우 보안 위협에 노출되므로 상위버전으로 교체·사용하여 보안 사고 사전 예방

다. 대상 PC

- MS Windows XP 이하 버전을 사용 중인 PC
 - MS Windows XP, Windows ME, Windows 98, Windows 95 등
- MS Office 2003 이하 버전을 사용 중인 PC
 - MS Office 2003, Office XP, Office 2000, Office 97 등

라. 사용현황

(2013.03.현재)

컴퓨터 운영체제	개 수	오피스 프로그램	개 수
Windows XP 이전	73,641(84.4%)	Office 2003 이전	17,295(17.0%)
Windows Vista	174(0.2%)	Office 2007	73,497(72.2%)
Windows 7	13,471(15.4%)	Office 2010	10,984(10.8%)
계	87,286(100%)	계	101,776(100%)

마. 컴퓨터 운영체제 및 오피스 프로그램 교체

- 모든 PC의 운영체제 및 오피스 프로그램을 교체 : 2014. 3. 31.까지
 - 운영체제 : Windows 7로 교체(Windows Vista는 그대로 사용 가능)
 - 오피스 프로그램 : Office 2007 또는 Office 2010으로 교체

바. 행정사항

- 신규 구입 PC는 컴퓨터 운영체제를 반드시 Windows 7 이상으로 설치하여 사용하고, Windows XP로 다운그레이드 금지

11. 인천광역시교육청 웹메일시스템 운영

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제38조(전자우편 보안대책)
- 인천광역시교육청 웹메일시스템 운영 및 상용이메일 차단 안내
(정보직업교육과-1374, 2010. 9. 20.)
- 웹메일시스템 기관업무용 메일 가입 안내
(정보직업교육과-8368, 2010. 12. 20.)

나. 목적

- 메일에 의한 해킹시도 및 워바이러스 감염 등이 증가함에 따라 상용이메일의 접속을 차단하고, 우리교육청에 최적화한 웹메일시스템 구축으로 사용자간 손쉬운 의사소통 및 정보교류

다. 가입 대상

- 인천광역시교육청 교직원 전체(각급학교 포함)

라. 개인 및 기관업무용 메일 회원가입 절차

- ① 사이트 주소 : <http://mail.ice.go.kr>
- ② 회원가입을 클릭하여 가입동의서를 확인하고 동의
- ③ 기본정보 및 인증서 등록 후 사용
 - ※ 기관업무용 메일 휴면계정에 대하여 SMS 발송을 위해 휴대전화번호 입력 필요(주 사용자 휴대전화 번호 입력)

마. 특수목적용(기관메일용) 인증서 발급 신청 방법

- ① 시교육청 홈페이지(www.ice.go.kr) → 행정정보 → 정보참고 메뉴에서 "전자서명인증서 신청서 변경 및 발급 절차 안내" 제목의 게시물 선택
- ② "공인인증서 신청서 서식.zip" 파일을 다운로드하여 압축 해제
- ③ "공인인증서 신청서 서식" 폴더의 "업무용 신청서.hwp"를 작성하되 **업무명에 기관 대표 메일**이라고 기입하여 시교육청 **정보지원과로 공문 발송**

바. 공직자 발송메일 보안관리 강화

- 공직자 발송 메일을 무단 열람하는 해킹사고가 지속적으로 발생
- 상용메일을 통해 업무자료가 송신되지 않도록 주의
- 메일 송·수신 또는 시의회 자료 제출은 반드시 우리 교육청 웹메일 사용

12. 웹사이트 접근 및 응용 프로그램 차단

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제30조(인터넷PC 보안관리), 제38조(전자우편 보안대책), 제40조(악성코드 방지대책)
- 상용 메신저 및 인터넷 자료공유 사이트 접속차단 강화 알림 (정보직업교육과-10964, 2012. 10. 09.)

나. 목적

- 상용 웹하드(클라우드) 및 메신저 서비스를 활용하여 업무 자료를 외부에서 열람·편집·전송하는 사례가 증가함에 따라 기관이 보유한 비공개, 비밀, 개인정보 등에 대한 중요자료 유출 방지
- 악성코드 유포지로 이용되는 자료공유 사이트 접속 차단으로 DDoS 공격용 악성코드 감염 및 좀비PC화 방지

다. 차단 현황

(2013.03.현재)

구분	유해사이트 (음란, 도박)	게임	P2P/ Warez	웹하드/ 클라우드	상용 이메일	상용 메신저
본청	차단	차단	차단	차단	차단	차단
교육지원청	차단	차단	차단	차단	차단	차단
사업소	차단	차단	차단	차단	차단	차단
각급학교	차단	차단	차단	차단	허용	차단

라. 접속 차단·해제 요청

- 특정 웹사이트 및 응용 프로그램의 접속 차단 또는 해제가 필요한 경우 [별첨]"웹 사이트/응용 프로그램 접속 차단·해제 요청서"를 작성하여 시교육청 정보지원과로 공문 발송
 - 양식 : ISAC사이트 [보안정보]-[참고자료실] 4번 게시물
- 접속 해제 요청에 대한 허용 사례
 - 스마트교육 관련 연구학교 등 부득이하게 대용량자료의 공유가 필요한 경우 기관장 책임하에 웹하드/클라우드 사이트 차단 해제
 - 특성화 교육, e-스포츠 게임 대회, 학교 축제 등으로 필요한 경우 웹게임 사이트 차단 해제
 - 이외 학교 수업 또는 업무에 반드시 필요한 경우

웹 사이트 / 응용 프로그램 접속 차단 · 해제 요청서

신청자 성명		직급 / 직위	
소속 (부서)		연 락 처	
구 분	<input type="checkbox"/> 차단 <input type="checkbox"/> 해제 (<input type="checkbox"/> <input checked="" type="checkbox"/>)		
	<input type="checkbox"/> 웹 사이트 <input type="checkbox"/> 응용 프로그램 <input type="checkbox"/> 웹 사이트 및 응용 프로그램		
요 청 대 상	웹 사이트	http://	
	응용 프로그램	(응용 프로그램 범주 및 프로그램 명)	
요 청 기 간	201 ~ 201		
차단 · 해제 대상 기관(부서)	ex) ○○교육지원청 ○○과 / ○○고등학교		
요 청 사 유			
처 리 일 자		처 리 자	(서명)

■ 위 요청 대상(웹 사이트 / 응용 프로그램)은 요청사유에 한하여 사용할 것이며 비공개, 비밀, 개인정보 등 중요자료 유출 시 발생하는 문제에 대하여 모든 책임을 질 것을 서약합니다.

신청일자 : 20

신 청 자 :

13. 「학교홈페이지 통합 구축」 사업

가. 관련

- 학교홈페이지 통합 구축 계획(정보직업교육과-9317, 2012. 5. 14.)

나. 배경 및 필요성

- (공공기관의 의무) 단위학교까지 홈페이지 장애인 웹 접근성 구현, 개인정보보호법 시행에 따른 고유식별정보(주민등록번호, 여권번호 등) 암호화, 주민등록번호 대체 수단 도입(공공 I-PIN등) 및 접속기록 보관 조치
- (교원 업무 증가) 학교의 홈페이지 개발·운영, 정보보안, 개인정보보호, 각종 정보화 사업으로 인하여 정보화 담당교사의 업무 증가
- (예산 중복 투자 방지) 사회·제도적 의무 이행사항 조치 및 최신 IT환경 조성을 위해 단위학교별 예산 투입에 대한 중복 투자 방지
- (급변하는 IT 환경 대응) 스마트기기 보급 저변화에 따른 최신 IT환경을 통한 정보 전달 및 SNS 요구 증가
- (홈페이지 보안 위협) 해킹, DDoS, 중요자료 유출 등 홈페이지 보안 위협 증가

다. 사업규모

연도	구분	내용	대상	비고
2012	서비스 기반 구축	○ 인프라 구축 (H/W 및 S/W)	본청	사업완료
	홈페이지 통합 구축	○ 홈페이지 구축·운영	144(6)	
2013	서비스 확산	○ 홈페이지 구축·운영 확대	208교	당해사업
2014	구축완료 및 안정화	○ 홈페이지 구축 완료	136교	
합계			488(6)	

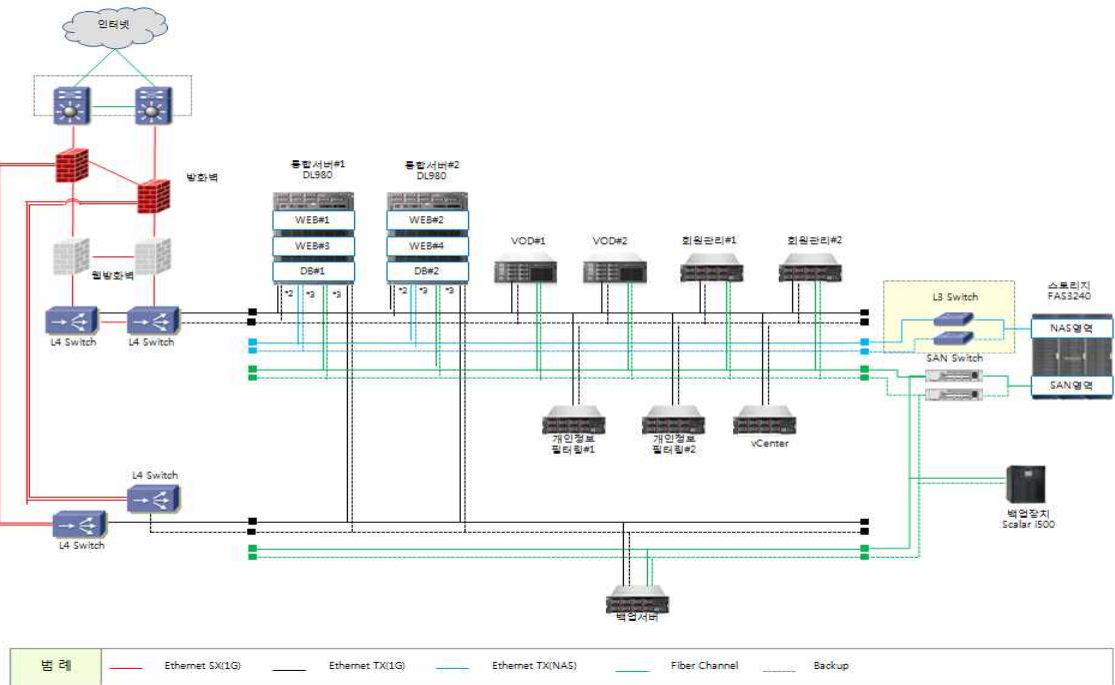
※ 대상 학교수는 2011. 9월 기준, 2013년 신설교는 본청에서 구축

※ ()는 본청 부서 홈페이지 구축 건수

라. 사업 목적

- 구축 완료한 홈페이지 통합 시스템을 확대·운영함으로써 학교의 서버관리 및 홈페이지 운영상 발생하는 예산 및 교사 업무 경감
- 개인정보보호 및 정보보안 관련 전문인력 부재에 따른 해킹 및 개인정보 노출에 대한 위협 해소

※ 시스템 구축 개념도



바. 향후 추진일정

- 2013년 홈페이지 통합 구축 2차 대상 학교 선정 : 2013. 2. 25.
- 2013년 홈페이지 통합 구축시 학교 요구사항 취합 : 2013. 3월
 - ※ 사업자 선정후 통합 홈페이지 운영 및 개발 자문위원단 운영
- 학교 홈페이지 통합 구축 2차 사업 계획 수립 : 2013. 4월초
- 학교 홈페이지 통합 구축 2차 사업 일상감사 의뢰 : 2013. 4월초
- 학교 홈페이지 통합 구축 2차 사업 계약 의뢰 : 2013. 4.중순
- 학교 홈페이지 통합 구축 2차 사업자 선정 : 2013. 6월
- 학교 홈페이지 통합 구축 2차 사업 실시 : 2013. 6월 ~ 10월

사. 학교홈페이지 통합 구축 주요 내용

○ 학교별 홈페이지 도메인 변경

구분	도메인 구성 규칙	비고
유치원	학교계정.icekg.kr	
초등학교	학교계정.icees.kr	
중학교	학교계정.icems.kr	
고등학교	학교계정.icehs.kr	
특수학교	학교계정.icesc.kr	
본청 각과	계정.ice.go.kr	

※ 학교계정은 현재 쓰고 있는 학교도메인의 고유 이름으로 함.

○ 홈페이지 구축 기본 방향

- (메뉴 구성) 홈페이지의 공통 메뉴를 기본으로 개발하되 대상 기관 현행 홈페이지를 기본으로 함
- (웹 어플리케이션 개발) 웹페이지 정형화 모듈 개발, 방과후학교 수강신청, 온라인투표, 인트라넷(일정관리), 예약 프로세스, 특화 게시판(과제물 제출, 토론 게시판 등)
- (디자인) 기본 템플릿 선택 후 학교 요구사항 반영
 - ※ 플래시는 사용금지 원칙(웹접근성 구현시 제약)
- (자료 이관) 현행 홈페이지 게시판의 2년간 데이터
 - ※ 전체 데이터 이관시 개인정보파일 유·노출 발생, 과거 불필요한 자료 탑재에 따른 저장 공간 낭비 등
- (지원센터 운영) 교육청, 사업자, 학교 간 원활한 의사소통 및 요구사항 반영 Feed-Back을 위한 유선 및 지원 홈페이지 운영
- (회원관리) 회원가입 수단 다양화(공공 I-PIN, ID-Password, 공인인증서 등)
 - ※ 고유식별정보(주민등록번호, 여권번호, 운전면허번호) 수집 및 사용 금지
 - ※ 홈페이지 원활한 운영을 위해 학생의 공공 I-PIN 발급 활성화 노력 (학생 1인당 1개 공공 I-PIN 갖기)
- (기존 홈페이지 처리방안) 신규 홈페이지 개발 완료시 기존 홈페이지는 사용 중지 권장
 - ※ 신규로 구축된 도메인에 대한 포털사이트(다음, 네이버 등) 등록은 학교 홈페이지 개통 일정에 맞추어 본청에서 일괄로 등록

※ 기존 도메인은 해지 또는 재사용 등 학교 사정에 따라 적의 조치

○ 학교 홈페이지 개발 프로세스



○ 개인정보보호 및 정보보안 시스템 구축 운영

- (개인정보필터링 시스템) 홈페이지 게시판에 개인정보(주민등록번호, 여권번호, 핸드폰, 이메일 등) 탑재시 자동 차단
- (웹방화벽) 웹어플리케이션 공격 탐지·차단
- (DB 암호화) 회원 비밀번호 및 개인정보 항목 암호화 저장
- (예상되는 문제점) 각종 보안장비 운영으로 홈페이지 보안은 강화되나 운영시 각종 제약 사항 발생

○ 학교 홈페이지 통합 지원 센터 운영

- (역할) 학교홈페이지 통합 구축시 학교 와 사업자간 의사소통, 사업완료 후 홈페이지 개선 및 교육 등 유지보수 담당

설치기관	주요 업무	인원	비고
본청	<ul style="list-style-type: none"> · 운영지원 홈페이지 운영(유선 콜센터 검임) · 학교홈페이지 신설, 개편, 폐지 시행 · 각급학교 요구 사항 지원 및 처리 <ul style="list-style-type: none"> - 게시판 생성, 디자인 변경 등 · 학교홈페이지 제작 시스템 사용법 지원 · 사용자 만족도 조사(매년 1회 이상) 	3명 (업체 상주인력)	

아. 기대효과

- 학교 홈페이지 통합관리로 담당교사 업무 경감 및 시스템 안정성 확보
- 장애인 웹 접근성 보장
- 회원정보 암호화 등 개인정보 보호 강화로 개인정보 유출 방지
- 홈페이지 보안 강화로 해킹, 분산서비스공격(DDoS) 등 사이버 침해 예방
- 홈페이지 재구축(개선) 및 유지보수 비용 절감

14. 웹 접근성(Web Accessibility) 이용 편의 제공

가. 관련

- 「국가정보화기본법」 제32조(장애인·고령자 등의 정보 접근 및 이용 보장)
- 「장애인차별금지 및 권리구제 등에 관한 법률」 제21조 및 동법 시행령 14조
- 「장애인복지법」 제22조(정보에의 접근)

나. 웹 접근성이란?

- 웹 사이트에서 제공하는 정보를 장애인, 노인 등이 비장애인과 동등하게 접근하고 이용할 수 있도록 웹 사이트 접근 환경 및 수준을 보장하는 것

다. 웹 접근성 준수 의무화

- 2008. 4. 11.부터 시행된 「장애인차별금지 및 권리구제에 관한 법률 시행령」 제14조에 의거하여 웹 접근성 준수가 단계적으로 의무화되었음
- 주요 적용 사이트 : 공공 및 민간 웹사이트

라. 교육기관의 단계적 범위

(「장애인차별금지 및 권리구제 등에 관한 법률 시행령」 제9조)

행위자 기간	교육기관(책임자)	문화예술체육
1년 이내 (‘09)	<ul style="list-style-type: none"> • 국·공·사립 특수학교 • 특수학급이 설치된 국·공립학교 • 장애전담 보육시설 	
2년 이내 (‘10)		<ul style="list-style-type: none"> • 국립중앙도서관 • 공공도서관
3년 이내 (‘11)	<ul style="list-style-type: none"> • 국공립유치원 • 초·중·고 대학교 • 보육시설(100인 이상) 	
5년 이내 (‘13)	<ul style="list-style-type: none"> • 사립유치원 • 평생교육시설, 연수기관 • 직업훈련기관(1000m² 이상) • 보육시설(100인 이하) 	<ul style="list-style-type: none"> • 체육관련 행위자

마. 「한국형 웹 콘텐츠 접근성 지침 2.0」 국가 표준(KICS) 제정

- 행정안전부에서는 국제표준과 웹 관련 신기술을 반영하여 「한국형 웹 콘텐츠

접근성 지침 2.0」 국가 표준(KICS)을 제정하였으며,

- 2011년 1월 1일 이후 추진되는 웹 사이트 개발 사업에는 각급기관 웹사이트 운영 시 개정된 지침을 적용
- 4개 원칙(Principle), 13개 지침(Guideline), 22개 검사항목(Checklist)로 구성
 - ※ 지침 전문 : 정보공유 침해대응 시스템(<http://isac.ice.go.kr>) [공개자료실] 19번 게시물 참고

바. 「모바일 애플리케이션 접근성 지침」 제정

- 행정안전부에서는 장애인·고령자 등이 모바일 서비스를 편리하게 이용할 수 있도록 모바일 애플리케이션 개발 시 준수해야 하는 세부사항을 반영하여 「모바일 애플리케이션 접근성 지침」을 제정
 - ※ 지침 전문 : 정보공유 침해대응 시스템(<http://isac.ice.go.kr>) [공개자료실] 30번 게시물 참고

사. 웹 접근성 자가 진단 매뉴얼 및 자동평가도구(K-WAH 3.0) 안내

- 「한국형 웹 콘텐츠 접근성 지침 2.0」 제정에 따른 웹 접근성 자가진단 매뉴얼 및 자동평가 도구(K-WAH 3.0)을 안내 하오니, 웹 접근성 지침 준수 기관에서는 참고하여 자율적인 개선이 이루어 질 수 있도록 협조
- 자동평가도구(K-WAH 3.0)는 웹 접근성 연구소(<http://www.wah.or.kr>)를 통해 K-WAH 3.0 프로그램 및 사용자 가이드를 다운로드 받을 수 있음

자. 행정사항

- 웹 접근성 기 준수 기관에서는 웹 사이트 유지보수 등을 통해 개정된 「한국형 웹 콘텐츠 접근성 지침 2.0」의 신규 내용을 단계적으로 적용
- 신규 홈페이지 구축 시 자동평가도구(K-WAH 3.0)를 이용하여 평가 결과 확인 후 개선 조치 수행
 - ※ 웹 접근성 미준수로 시정 명령을 받은 기관에서 재차 미이행시 3천만원 이하의 과태료에 처함

차. 참고 사이트 및 자료

- 한국정보화진흥원 웹접근성 연구소(<http://www.wah.or.kr>)
- 웹 접근성 향상 캠페인(<http://www.wah.or.kr/campaign>)

15. 보안서버 구축

가. 관련

- 개인정보보호법 제29조(안전조치의무) 및 동법 시행령 제30조(개인정보의 안정성 확보 조치)
- 각급기관 운영 홈페이지 보안서버 및 I-PIN 구축 안내 (정보직업교육과-1770, 2012. 2. 14.)
- 각급기관 홈페이지 운영 현황 제출(정보지원과-1658, 2013. 2. 5.)



나. 보안서버란?



- 보안서버란 인터넷상에서 사용자 PC와 웹서버 사이에 송·수신되는 개인정보를 암호화하여 전송하는 서버를 의미
- 개인정보를 송·수신하는 대표적인 예로는 회원 가입 시 주민번호 입력, 로그인시 ID/패스워드 입력 등이 해당됨
- 인터넷 상에서 암호화되지 않은 개인정보는 가로채기 등의 해킹을 통해 쉽게 해커에게 노출될 수 있으므로, 웹서버에 보안서버 솔루션을 설치하면 해커가 중간에 데이터를 가로채도 암호화되어 있어 개인정보 노출 방지
- 보안서버는 별도의 서버(H/W)를 새로 구축하는 것이 아니라 현재 웹서버에 SSL 인증서(보안서버)를 발급받아 설치하거나 응용 프로그램을 설치
- 대상기관 : 교육청 및 산하기관, 각급학교 등

다. 보안서버의 종류

- 보안서버는 구축 방식에 의해 크게 [SSL 인증서를 이용한 보안서버]와 [암호화 응용 프로그램을 이용한 보안서버]로 구분

SSL(Secure Socket Layer)방식	응용프로그램 방식(표준보안API)
<p>웹서버와 웹브라우저에 별도의 보안프로그램 설치가 필요없으며, 웹서버에 설치된 SSL인증서를 사용하여 개인정보를 암호화하여 전송</p>	<p>웹서버에 접속하면 사용자 컴퓨터에 자동으로 보안 프로그램이 설치되고 이를 통해 개인정보를 암호화하여 전송</p>
<p>[https://도메인명]</p>	<p>[인증서 로그인]</p>
	

라. SSL 인증서와 표준보안 API 개요

- SSL 방식은 웹브라우저와 서버간의 통신에서 정보를 암호화함으로써 악의적 공격자가 해킹을 통해 사용자의 정보를 유출하더라도 사용자 정보의 내용을 보호할 수 있는 기능을 갖춘 보안 솔루션
- 표준보안 API는 SSL 방식에서 제공하는 보안서비스를 동일하게 제공하며 그 외에 SSL 인증서 방식에서 제공하지 못하는 사용자의 신원확인, 사용자의 인증 및 부인 방지 기능까지 추가적으로 제공
- 표준보안 API는 신원확인이 필요한 업무시스템에서 업무담당자의 신원확인을 ID/PW로 하는 경우 인증서 기반의 신원확인(API) 시스템을 구축하여야 함
예) 업무담당자 로그인 사이트 등(초·중·고등학교인 경우 해당 사항 없음)

구분	SSL 인증서	표준보안 API
발급대상	교육부 및 직속기관, 연구·출연기관, 국·공립·사립대학, 교육청 및 산하기관, 각급학교 등	
신청처	교육청 및 산하기관, 각급학교 → 시교육청(공문제출)	교육부 전자서명인증센터 [한국교육학술정보원] (☎ 02-2118-1755)
기술지원	교육부 전자서명인증센터	
발급비용	무료	무료
주요기능	데이터 암호·복호화	데이터 암호·복호화 전자서명, 사용자 인증, 실명확인
구축 가능 웹서버	Apache, WebToB, Iplanet, IIS, Tomcat, Weblogic, IBM-HTTP, Oracle-HTTP 등 연동 Web Browser : Internet Explorer, Chrome, Opera, Safari	Windows Server, SunOS, linux, IBM AIX, HP-UX

마. SSL 보안서버 구축 현황

(2013. 2. 기준)

구분	대상도메인	구축완료도메인	구축율(%)	비고
본청	20	14	70%	
교육지원청	23	21	91.3%	
사업소	19	18	94.7%	
초중고특수	510	473	92.7%	
합계	572	526	92%	

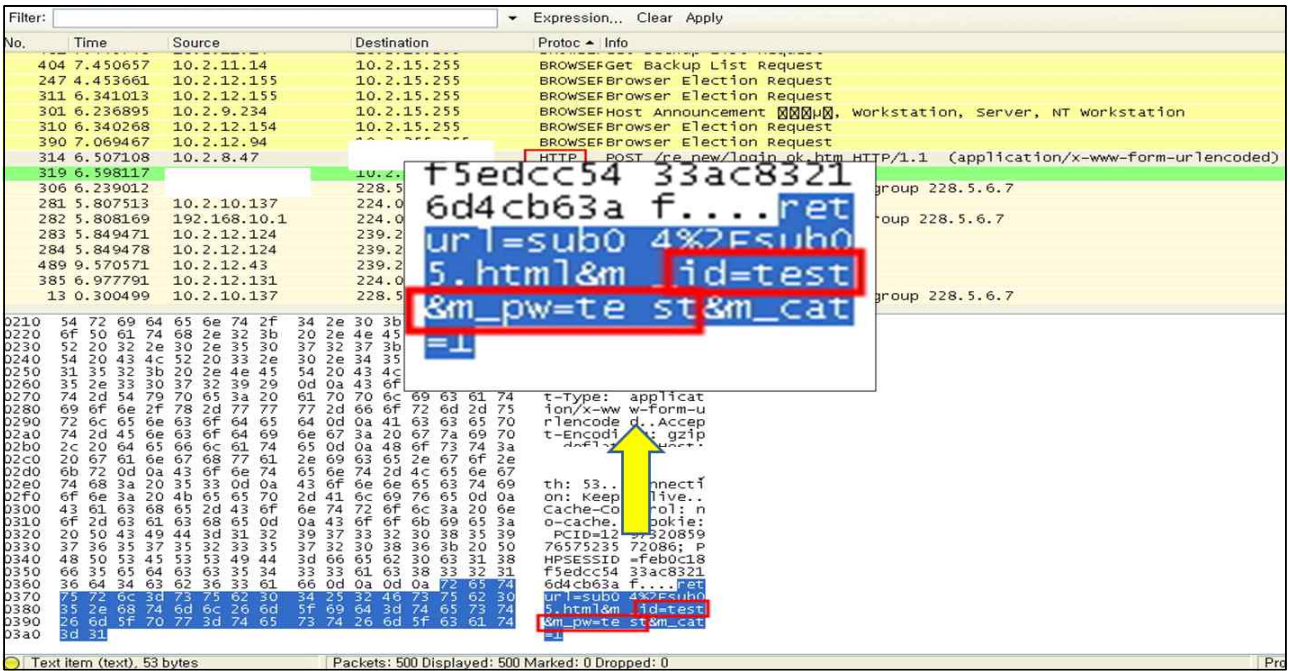
※ SSL인증서는 도메인 기준으로 발급됨

바. SSL 인증서를 이용한 보안서버 구축 시 유의 사항

- 서비스 성능을 고려할 때 웹 서비스 전 구간을 암호화하기 보다는 선별적인 서비스 사용이 필요함
- 웹 사이트 전반적으로 중요 정보 전송 구간(주민번호, ID/PW 등)을 확인하여 암호화 구간을 확정하고, 중요 정보 전송 구간의 http 서비스를 차단하여 https 서비스만 가능하도록 조치하여야 함

○ 내부망에서 운영 중인 정보시스템에 대해서도 보안서버 구축

- ※ 중요 정보 전송 구간에 http와 https를 동시에 서비스하여 평문 전송과 암호문 전송이 모두 이루어지는 경우가 다수 발생
- ※ 평문 전송 시(http 통신 구간) 패킷 스니핑(데이터 훔쳐보기)을 시도 하였을 때 중요 정보가 그대로 노출됨을 확인 할 수 있음(ID : test, PW : test)

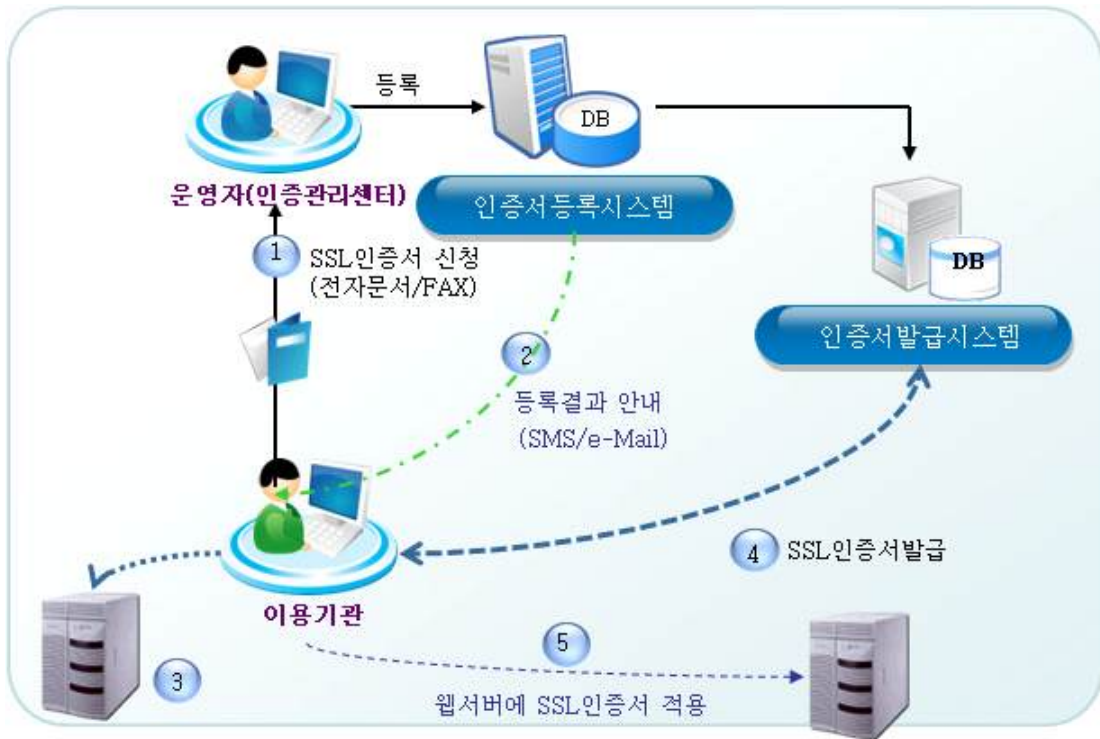


사. 행정사항

- 보안서버 미적용 기관에서는 즉시 완료될 수 있도록 적극 협조
 - ※ 미적용시 3천만원의 과태료 부과
- 보안서버를 구축한 기관에서는 실제 https 서비스 구간에 암호화된 데이터들이 전송되는지 보안서버 구축 유지보수 업체를 통하여 점검 요청
- 신규 홈페이지 구축 시 보안서버 구축 완료 후 홈페이지 개통

아. 보안서버 구축 절차(SSL 인증서를 이용한 보안서버 구축)

- ① 인증서 신청서(별첨양식)를 작성하여 시교육청 정보지원과로 전자문서 제출
- ② 전자서명인증센터(www.epki.go.kr)에서 신청자에게 SSL인증서 발급 이메일 발송
- ③ 신청자는 적용할 웹서버에서 인증요청정보(CSR)파일 생성
 - ※ CSR(Certificate Signing Request) : 인증서 서명 요청



- ④ 생성된 인증요청정보(CSR) 파일을 이용하여 전자서명인증센터에서 SSL인증서 발급
- ⑤ 발급받은 SSL인증서를 운영 중인 웹서버에 적용
 - ※ 신청서양식 및 보안서버 구축가이드는 교육부 전자서명인증센터 자료실에서 다운로드하여 활용
 - ※ 보안서버 기술지원 콜센터(전자서명인증센터) ☎ 02-2118-1755

자. 참고 사이트 및 자료

- 교육부 전자서명인증센터 (<http://www.epki.go.kr>)

16. 공공 I-PIN 서비스 도입

가. 관련

- 「개인정보보호법」 제24조(고유식별정보의 처리제한) 및 같은법 시행령 제21조(고유식별정보의 안전성 확보조치)
- 각급기관 운영 홈페이지 보안서버 및 I-PIN 구축 안내 (정보직업교육과-1770, 2012. 2. 14.)
- 각급기관 홈페이지 운영 현황 제출(정보지원과-1658, 2013. 2. 5.)

나. 공공 I-PIN이란?

- 공공 I-PIN은 Internet Personal Identification Number의 약자로, 인터넷상 개인 식별번호를 의미하며, 홈페이지 회원가입, 글쓰기 시 주민등록번호를 사용하지 않고도 본인임을 확인할 수 있는 개인정보보호 서비스임

다. 공공 I-PIN 적용 대상

- 개인정보보호법 제24조(고유식별정보의 처리 제한)에 따라 본인확인 등 회원제 서비스 구축·운영 시 공공 I-PIN 적용이 의무화
- 웹 사이트 회원가입 시 또는 게시판 글쓰기 시에 고유식별정보를 사용(입력)하는 경우
 - ※ 고유식별정보 : 주민등록번호, 여권번호, 운전면허등록번호, 외국인등록번호

라. 공공 I-PIN 구축 현황(2013. 2. 기준)

구 분	공공 I-PIN 구축 대상기관 수	공공 I-PIN 구축 기관 수	구축율(%)	비 고
본청	10	9	90%	
교육지원청	8	7	87.5%	
사업소	13	13	100%	
초·중· 고·특수	175	175	92.3%	
합 계	206	204	99%	

마. 공공 I-PIN 보급(적용) 참고사항

- 공공 I-PIN 적용 시 홈페이지 수정이 불가피하므로, 홈페이지 유지보수 업체와 사전에 협의토록 함
- 공공I-PIN 적용을 위한 서버용 인증서 발급은 인증서 신청서(별첨 양식)를 작성하여 정보지원과로 공문(전자문서)으로 제출 신청, 전자서명인증센터(<http://www.epki.go.kr>)에서 참조번호/인가코드 입력 후 발급
 - ※ 미적용시 3천만원의 과태료 부과
- 보급 지원 : 공공I-PIN센터(공무원창구) (gpin.go.kr:8080)
☎ 02-3279-3480~2

바. 참고 사이트 및 자료

- 교육부 전자서명인증센터(<http://www.epki.go.kr>)

<교육행정전자서명인증서 신청양식 : 2-2(기관용-서버용, SSL용)>

교육행정전자서명 인증서 신청서 (기관용) <input type="checkbox"/> 서버(컴퓨터)용 <input type="checkbox"/> SSL용			
소속(기관명)		기관코드	
사업자등록번호			
인증서활용용도			
인증서관리담당	성명	전화번호	
		휴대전화번호	
	이메일	팩스번호	
신청구분	신청종류	<input type="checkbox"/> 신규 <input type="checkbox"/> 재발급 <input type="checkbox"/> 폐지 <input type="checkbox"/> 효력정지 <input type="checkbox"/> 효력회복	
	재발급·폐지사유	<input type="checkbox"/> 인증정보 노출 <input type="checkbox"/> 소속기관 변경 <input type="checkbox"/> 저장매체파손 또는 비밀번호 분실 <input type="checkbox"/> 기타 ()	
사용시스템	운영체제	<small>* 예시 : Solaris2.7, Windows 2003</small> WEB/WAS	<small>* 예시 : webtob</small>
	IP 주소	<small>* 예시 : 152.99.1.1</small> 도메인명	<small>예시 : www.epki.go.kr</small>
임시비밀번호	* 반드시 8자리 숫자 기입(영문자 사용불가)		
개인정보취급	※ 개인정보보호법 제15조 1항(개인정보의 수집·이용)에 의거하여 본인의 개인정보를 제공할 것을 <input type="checkbox"/> 동의합니다. <input type="checkbox"/> 동의하지 않습니다.		
상기와 같이 교육행정전자서명 인증서서비스를 신청합니다. 교육부 전자서명인증센터 인증업무세부지침을 준수하며, 본 신청서 관련 정보를 전자인증 및 행정정보공동이용 업무에 활용하는 것에 동의합니다.			
담 당 자 :		서명 또는 (인)	
위와 같이 교육행정전자서명 인증서 신청을 확인합니다.			
		년 월 일	
확인기관(부서)장 :		서명 또는 (인)	
교육부장관 귀하			

※ 공문서 붙임으로 본 신청서를 제출할 경우, 담당자 및 확인기관(부서)장 서명 또는 (인)은 생략 가능함.

【작성요령】

- ① 신청서 종류
 - 서버용 : 정보통신 장비에 활용하는 인증서
 - SSL용 : 웹서버에서 SSL 표준보안프로토콜을 활용하기 위한 인증서
- ② 소속(기관명) 및 기관코드 : 학교의 경우 상위기관과 학교명을 기재하고, 행정기관의 경우 “과”단위까지 기재한다. 기관코드는 행정안전부 행정표준코드에 등록된 해당 기관의 코드를 말하는 것으로서 행정표준코드관리시스템 (<http://code.gcc.go.kr>)에서 확인할 수 있다.
 [예] 서울특별시중부교육지원청 청운중학교, 교육부 교육기반통계국 교육정보화과
- ③ 인증서활용용도 : 인증서를 활용할 응용업무가 있는 경우 기재한다.
 [예] 나이스 대학업무시스템, 교육부 문서유통시스템 등
- ④ 인증서관리담당 : 기관용 인증서를 발급 받아 사용 및 관리하는 담당자에 대한 정보를 기재한다.
- ⑤ 신청구분 : 신청구분 항목을 선택하여 ‘√’ 또는 ‘■’로 표시하고, 재발급·폐지를 선택한 경우 재발급·폐지사유 항목을 선택하여 표시한다.
 - 인증정보노출 : 가입자 행정전자서명생성기가 노출되었거나 분실되었을 경우
 - 소속기관변경 : 부처간 인사이동이 있는 경우 기존 부처에서 인증서를 폐지, 신규 부처에서 신규 발급 신청을 해야 한다.
 - 저장매체파손 및 비밀번호 분실 : 행정전자서명키가 저장매체 파손, 인증서 사용 비밀번호 분실 등으로 행정전자서명키를 인식할 수 없는 경우
 - 기타 : 인증서 유효기간 만료 등 기타 사유를 기재
- ⑥ 사용시스템
 - 운영체제 : 인증서를 설치하여 사용할 컴퓨터의 운영체제를 말한다.
 [예] Solaris2.7, Windows 2003
 - WEB/WAS : 서버용/SSL용 인증서를 설치하는 WEB서버와 WAS서버를 기재한다.
 [예] WEBToB, Apache
 - IP 주소 : 서버용 인증서를 설치하는 컴퓨터의 네트워크 IP 주소를 기재한다.
 [예] 152.155.101.122
 - 도메인명 : SSL용 인증서를 설치하는 웹서버의 도메인명을 기재한다.
 [예] 일반 : www.epki.go.kr, 멀티 : www.epki.go.kr, www.mest.go.kr...
- ⑦ 임시비밀번호 : 인증서 발급시 활용하는 숫자 8자리를 반드시 기재한다.
 ※ 분실시 인증서 발급을 할 수 없음.

17. 웹취약점 점검 시스템 운영

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제32조(웹서버 등 공개서버 보안관리)
- 웹취약점 점검 시스템 운영 계획 알림(정보직업교육과-20018, 2012.10.12)

나. 목적

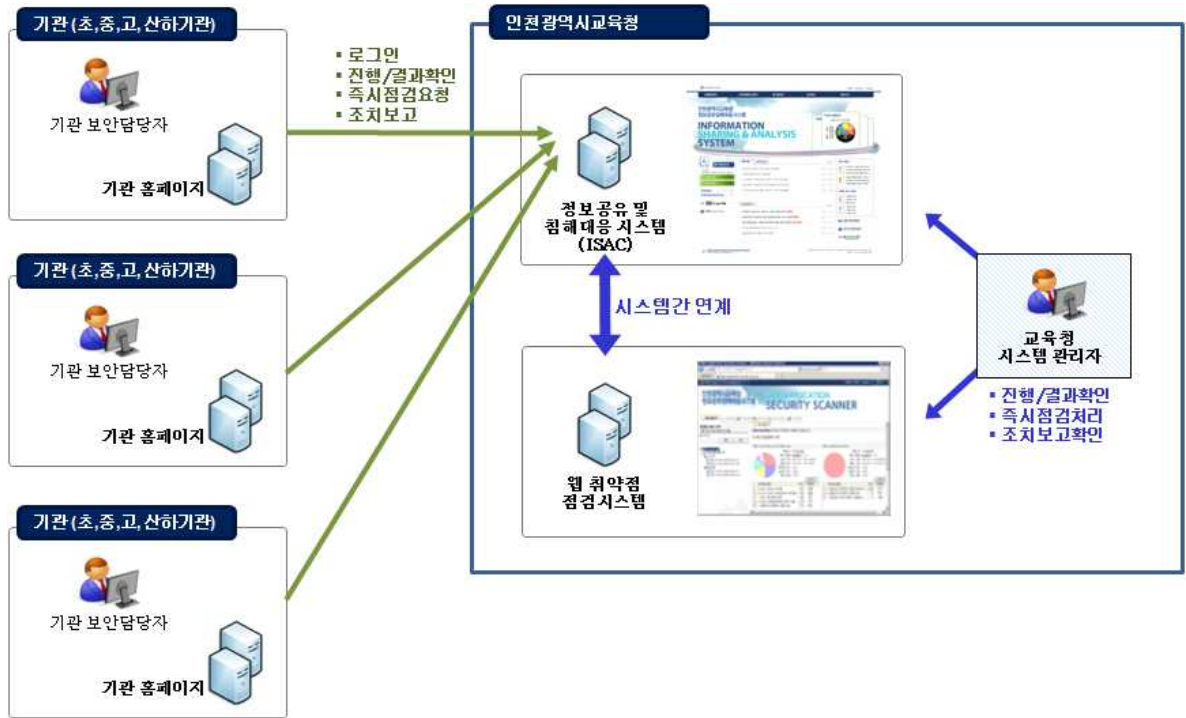
- 우리교육청 산하 각급기관 홈페이지의 취약점을 조기 발견하여 침해사고 사전 예방
- 개인정보 유출에 대비하여 데이터를 안전하게 보호하고 홈페이지 보안에 대한 관심 증대

다. 2013년 추진 계획

- 웹 서비스 취약점 점검
 - 대상 : 인천광역시교육청 소속 전 기관에서 운영 중인 홈페이지
(외부업체 호스팅 서비스 중인 기관 홈페이지 포함)
 - 일정 : 대상기관 전체에 대하여 연중 상시 점검
 - 내용 : 국가정보원 8대 취약점, 한국인터넷진흥원의 10대 취약점, OWASP TOP 10에 명시된 취약점 항목 등 잠재적 위험요소 점검
 - ※ 학교 홈페이지 통합 구축 대상학교는 시교육청에서 별도 점검 예정(2012년 150개 홈페이지)
- 점검 방법 : 웹 취약점 점검 S/W를 이용한 자동 점검
- 점검체계별 기능 및 역할

기관명	기능 및 역할	비고
인천광역시교육청	<ul style="list-style-type: none"> • 점검 일정 관리 및 진행·결과 확인 • 점검 실시 사전 안내 및 점검결과 통보 • 취약점 조치 결과 검토 	
대상기관	<ul style="list-style-type: none"> • 점검 전 사전 준비사항 이행 • 점검보고서 확인 및 취약점 보완 후 조치결과 보고 • 홈페이지 구축·개편 시 웹 취약점 점검 신청 	

○ 웹 서비스 점검 시스템 구성도



○ 취약점 점검 주기

- 정기 점검

- 1) 연 2회 정기 점검 실시
- 2) 각 기관에서는 점검 일정을 확인하여 점검 전 사전 준비사항 반드시 이행
- 3) 점검 일정에 따라 정보공유침해대응 시스템에 등록된 정보보안담당관에게 SMS 사전 통보

- 즉시 점검

- 1) 홈페이지 구축·개편 등으로 취약점 점검이 필요한 경우 해당 기관의 요청에 따라 즉시 점검 실시
- 2) 즉시 점검 요청은 정보공유침해대응시스템 웹취약점 점검 요청 메뉴 이용

○ 점검 일정

- 정기 점검 : 정보공유침해대응시스템 게시판을 통하여 사전 공지 예정이며, 각 기관별 일정표에 따라 순차적 점검

※ 추후 공문 시행 예정

- 즉시 점검 : 해당 기관의 즉시 점검 요청일

○ 취약점 점검 전 사전 준비사항

- 각 기관 홈페이지 URL 정비

- 정보공유침해대응시스템 홈페이지 운영 현황 홈페이지 주소 확인 후 URL 현행화

※ 정보공유침해대응시스템 - 로그인 후 우측 상단 My page - 홈페이지 운영 현황(사용자 정보의 소속기관명 확인)

- 홈페이지 개편 등으로 홈페이지 주소나 메인 페이지가 변경되거나 홈페이지 정보가 누락된 경우 정상적으로 진단되지 않을 수 있으므로 반드시 확인

- 점검 시작 전 홈페이지 데이터 백업 실시 : 홈페이지의 구조적 문제점이나 취약점 점검 도중 예상치 못한 오류 발생 등으로 인하여 데이터 손실이 발생 할 수 있으며, 이에 대비하여 점검 전 반드시 데이터 백업 실시

- 외부 호스팅 서비스 이용 기관은 해당 업체에 점검 일정 사전 통보

- 취약점 점검이 원활히 이루어 질 수 있도록 점검 일정에 따라 취약점 점검 서버 IP 예외처리(교내에 웹서버가 있는 경우는 해당사항 없음)

- 취약점 점검 서버 IP 정보

장비명	IP 정보	비고
웹취약점 점검 서버	125.133.128.201	
	125.133.128.202	
	125.133.128.203	

- 점검결과 확인 및 조치 결과 보고

- 이용자의 불편을 최소로 줄이고자 웹 취약점 점검은 이용자가 상대적으로 적은 야간에 실시함. 다만, 점검 다음 날 홈페이지의 정상적인 서비스 여부 확인이 필요함

- 정보공유침해대응시스템 웹취약점 점검 메뉴를 이용하여 점검 진행상태 확인 가능

- 각 기관의 홈페이지의 구조 및 데이터량에 따라 점검소요 시간은 각각 다르며 점검 완료 시간 예측에 어려움이 있음

- 점검완료 후 각 기관의 취약점 점검 보고서를 확인하여 홈페이지에 존재하는 취약점 제거 조치 실시

- 취약점 제거 조치 결과 보고

- 취약점 조치 결과는 점검 완료 시점으로부터 21일(3주) 이내에 조치 완료하여 정보공유침해대응시스템 웹 취약점 진단관리 메뉴를 통하여 보고
- 취약점에 대한 설명과 조치 방법에 대한 안내는 취약점 점검 보고서 참고

라. 행정사항

○ 점검 전 대상기관 사전 준비 사항 이행

- 1) 각 기관 홈페이지 URL 현행화
- 2) 점검 시작 전 홈페이지 데이터 백업 실시
- 3) 외부 호스팅 서비스 이용 기관은 해당 업체에 점검 일정 사전 통보

○ 점검결과 확인 및 조치

- 1) 점검 진행상태 확인 및 다음 날 홈페이지 정상 서비스 여부 확인
- 2) 점검완료 후 각 기관의 취약점 점검 보고서를 확인하여 취약점 제거 조치 실시

○ 취약점 조치 결과 보고

- 1) 점검 완료 시점으로부터 21일(3주) 이내에 취약점 조치 완료 보고
- 2) 취약점에 대한 설명과 조치 방법은 취약점 점검 보고서의 해설 참고
 - ※ 홈페이지 개편을 예정 중이거나 기타 불가피 이유로 기한 내에 조치가 불가능할 경우 향후 취약점 조치 계획(사유 포함)을 공문으로 제출

III 개인정보보호 업무 추진

1. 홈페이지 개인정보 유출 및 노출 방지 철저

가. 관련

- 민원인 핸드폰 번호 유출 민원(국민신문고, 2013.01.06.)
- 개인정보 노출점검 대상 홈페이지 수요조사 협조 요청
(행정안전부 개인정보보호과-599, 2013.02.14)
- 홈페이지 개인정보 노출 점검 결과 통보 및 조치결과 제출
(정보지원과-3742, 2013.3.11.)

나. 학교홈페이지 개인정보 노출 적발 현황

2009		2010		2011		2012		총계	
기관수	노출건수	기관수	노출건수	기관수	노출건수	기관수	노출건수	총기관수	총 노출건수
17	2,309	53	1,697	10	836	22	6,476	102	11,318

- 개인정보 노출 현황 분석
 - 개인정보 노출 경로 : 홈페이지(98%) 및 파일공유사이트(2%)
 - 개인정보 노출 건수 : 홈페이지(6,308건, 55.7%), P2P(5,010건, 44.2%)
 - 홈페이지 개인정보 노출 유형
 - 대부분 사용자 부주의로 인해 게시판에 개인정보 탑재
 - 업무용 PC 내 개인정보를 휴대용 저장장치를 통해 자택 PC에 저장 후 파일공유프로그램을 통해 유출
 - 무분별한 개인정보의 공유, 개인정보 수집 목적 외 이용, 권한 없는 자의 개인정보 접근
- 시사점
 - 개인정보 노출 경로는 홈페이지가 절대적 높임
 - 파일공유 사이트를 통한 개인정보 노출은 빈도는 낮으나 대량의 개인정보 유출 발생
 - 일반 국민은 자신의 개인정보의 관리에 매우 민감히 여기고 있으나 공공기관의 개인정보관리는 국민의 기대 수준에 미흡

2. 개인정보 노출 진단시스템 운영

가. 관련

- 「인천광역시교육청 정보보안 기본지침」 제33조(홈페이지 게시자료 보안관리)
- 개인정보 노출 예방을 위한 홈페이지 점검 안내
(정보직업교육과-12008, 2010.07.29)

나. 목적

- 교육청 산하 전체 기관 홈페이지의 개인정보 포함 여부를 주기적으로 진단하여 개인정보 침해사고를 사전에 예방하고자 함

다. 진단시스템 운영 현황

구분	등록 홈페이지 수	진단 홈페이지 수	비고
2011년	575	2,830	등록 홈페이지 수는 각 년도 말 기준
2012년	585	2,093	

라. 시스템 사용 유의사항

- 진단대상으로 등록되어 있는 기관 홈페이지 주소 확인
 - 홈페이지 개편 등으로 홈페이지 주소나 메인 페이지가 변경된 경우 정보지원과로 통보
- 주민번호 진단내역 중 실제 주민번호가 아닌 경우에도 조치 필요
 - 예시 주민번호, 일련번호로 된 파일명 등 수정(삭제) 조치
- 정기 진단시 전체 기관 진단주기를 고려하여 주민번호 항목만 진단하므로, 주기적으로 이메일, 핸드폰 등의 진단항목을 포함하여 즉시 진단 수행
 - 이메일, 핸드폰번호 등은 오탐 사례가 많으므로 유의
 - 즉시 진단은 등록된 순으로 순차적으로 진행되므로 즉시진단이 많은 경우 진단처리가 지연될 수 있음

마. 홈페이지 운영 조치사항

- 게시판별 담당자를 지정하여 홈페이지 자료 주기적으로 점검(월1회 이상)
- 단순 공지 등 불필요한 게시물 정기적으로 삭제 조치(연1회 이상)

- 웹서버에 I-Safer(개인정보 검색프로그램)를 설치하여 주기적으로 서버 내 파일 점검 수행 권장(윈도우 계열 서버만 가능)
- 회원가입, 게시물 작성 등 홈페이지 개인정보 입력(수집)항목은 최소한으로 제한
- 비공개 게시판을 포함한 홈페이지 모든 게시판에 개인정보 등이 포함된 중요자료 탑재 금지
- 개편 전 홈페이지는 일정기간만 병행 운영, 자료 백업 후 홈페이지 폐쇄 조치

바. 행정사항

- 주1회 이상 시스템 접속, 개인정보 노출 진단결과 확인
- 소속 교직원 및 학생 등을 대상으로 홈페이지 노출 예방 교육 실시

사. 홈페이지 개인정보 노출 사례

노출 유형	노출 내역	예방조치
사용자 부주의	구직 게시판에 사용자가 본인의 이력서를 게시함	개인정보 탑재 금지 안내 문구 게시
	학교 동아리 게시판에 학생 본인 개인정보가 포함된 대회 참가신청서를 게재함	
	학생이 본인의 개인정보가 포함된 독후감을 게재함	
홈페이지 설계 오류	이미지파일명을 주민번호로 설정하여 소스코드 기능을 통해 공개됨	비공개 게시판 소스코드 확인
	비공개 제증명 신청내용이 소스보기 기능을 통해 공개됨	
업무담당자 부주의	교육계획서에 학생 및 강사 개인정보를 포함하여 게재함	자료 게재 시 개인정보 포함 여부 확인 (양식, 계획서, 회의록 등)
	학생 개인정보가 포함된 대회 신청서, 추천서를 게재함	
	특강 원고자료에 강사정보를 포함하여 게재함	
	특별활동 지침서에 학생과 학부모 명단을 포함하여 게재함	
	유관기관에서 시행한 책임자 개인정보가 포함된 공문을 수정없이 게재함	엑셀자료의 경우 개인정보 검색프로그램(I-Safer) 반드시 확인한 후 게재
	필터기능이 적용된 수영대회 대진표 엑셀파일을 게재함 (필터 해제 시 참가학생 개인정보 표시)	
	반편성 엑셀자료가 학생 개인정보가 포함된 워크시트가 왼쪽에 숨겨진 채로 게재됨	
	문서정보(파일-문서정보)에 주민번호가 들어간 파일을 여러 사용자가 복사하여 중복 게재함	
	학교운영위원회, 이사회 회의록에 교직원 개인정보를 포함하여 게재함	

※ 노출사례 대부분 업무담당자 부주의에 의해 발생

⇒ 소속 교직원 대상 개인정보 노출 예방 교육, 자료 게재 시 확인 절차 필요

아. 개인정보 진단관리 등록

- 정보공유 침해대응시스템 (http://isac.ice.go.kr) 로그인
 - 위협정보관리 - 개인정보 진단관리 메뉴로 이동
 - 기관 홈페이지 등록
 - 진단URL, 사이트이름 입력 저장(홈페이지 운영현황이 등록된 경우 해당정보가 기본적으로 표시됨)
 - 진단URL은 도메인 입력, 도메인이 없는 경우만 IP로 입력
- ※ 기관에서 홈페이지를 여러 개 보유한 경우 해당 홈페이지 모두 등록

The image shows two screenshots of the '개인정보 진단관리' (Personal Information Diagnosis Management) registration form. The top screenshot shows the form with a red box around the '진단항목' (Diagnosis Items) section. The bottom screenshot shows the same form with a red box around the '진단항목' section and a note at the bottom.

개인정보 진단관리 > 등록

진단URL:

사이트이름:

포트: 80

기관: 인천광역시교육청 기관명 찾기

진단항목:

<input checked="" type="checkbox"/> 주민번호	<input type="checkbox"/> 카드번호	<input type="checkbox"/> 여권번호
<input type="checkbox"/> 면허증번호	<input type="checkbox"/> 핸드폰번호	<input type="checkbox"/> 전화번호
<input type="checkbox"/> 이메일	<input type="checkbox"/> 건강보험번호	<input type="checkbox"/> 은행계좌번호

스캔기간: 30일 즉시

동시접근수: 5

이메일수신: 수신

최대처리시간: 10 일

○ 30일 진단의 경우 전체기관의 진단 주기를 고려하여 주민번호만 진단 가능합니다. 다른 항목을 진단하시려면 즉시 진단을 선택하시고, 즉시 진단 요청이 많을 경우 순차적으로 처리되어 진단이 지연될 수 있음을 참고하시기 바랍니다.

자. 개인정보 진단내역 확인

- 로그인 후 메인페이지로 이동(상단 Home 클릭)
- "개인정보 진단내역 보기" 버튼 클릭 : 등록된 홈페이지의 진단내역 화면으로 이동

○ 진단내역 화면의 "진단결과" 버튼 클릭

※ 진단내용에 대상 URL 수가 "0" 또는 "1"로 나온 경우는 진단이 제대로 수행되지 않은 경우이므로 시교육청으로 문의

The screenshot shows the 'Information Sharing & Analysis System' dashboard. A table titled '과거 진단 내역' (Past Scan History) is visible, with columns for '진단 URL' (Scan URL), '시작일' (Start Date), and '완료일' (Completion Date). A red box highlights the '진단결과' (Scan Results) button. The table contains the following data:

진단 URL	시작일	완료일
http://	2013-03-26 18:02:30	2013-03-26 18:51:42
http://	2013-03-25 20:55:39	2013-03-25 22:30:32
http://	2013-03-25 12:39:31	2013-03-25 20:55:31
http://	2013-03-25 13:00:08	2013-03-25 20:42:58
http://	2013-03-25 16:09:17	2013-03-25 20:42:34
http://	2013-03-25 16:32:44	2013-03-25 20:28:04
http://	2013-03-25 00:55:23	2013-03-25 16:45:20
http://	2013-03-24 16:26:33	2013-03-25 16:28:03
http://	2013-03-25 15:34:44	2013-03-25 16:27:21
http://	2013-03-24 16:29:23	2013-03-25 16:09:06
http://211.43.130.35/main/main.htm	2013-03-24 18:01:43	2013-03-25 15:34:42
http://www.yslib.so.kr	2013-03-24 16:44:16	2013-03-25 14:02:57
http://www.huieong.es.kr/usr/mav/MainView.do2013-03-25	10:43:36	2013-03-25 12:39:20

○ 진단결과 보고서 확인 : 항목별로 노출된 건수가 있는 경우 왼쪽 해당 진단항목 클릭

The screenshot shows the '개인정보 노출 현황' (Personal Information Exposure Status) report. A table displays the following data:

진단 URL	http://www
진단 완료 일자	2013년 03월 25일 20시 42분
전체 URL	18743 건
개인정보 노출 URL	6 건
개인정보 미노출 URL	16907 건

Below the table is a bar chart titled '개인정보 노출 현황 그래프' (Personal Information Exposure Status Graph). The x-axis lists various personal information items, and the y-axis shows the count. The '주민등록번호' (Residential Registration Number) bar is highlighted with a red box and has a value of 6.

개인정보 항목	노출 건수
주민등록번호	6
카드번호	0
여권번호	0
운전면허번호	0
휴대폰번호	0
일반전화번호	0
이메일	0
건강보험번호	0
은행계좌번호	0
홈페이지 진단현황	0
진단대상 URL	0
진단 예외 URL	0
미검증 URL	0
외부도메인 현황	0

○ 노출 여부 확인 후 조치 : 보고서의 노출URL을 클릭하면 해당 경로로 이동

※ 상단 "엑셀", "PDF" 아이콘 클릭 시 보고서 다운로드 가능

인천광역시교육청 U-PRIVACY SAFER SCANNER

진단결과 보고서 - http://www. [뒤로가기]

개인정보 노출현황

- 주민등록번호
- 신용카드번호
- 여권번호
- 운전면허번호
- 휴대폰번호
- 일반전화번호
- 이메일
- 건강보험번호
- 은행계좌번호

홈페이지 진단현황

- 진단대상 URL
- 진단 예외 URL
- 미 검증 URL

주민등록번호 검출

진단 URL	http://www
진단 완료 일자	2019년 03월 25일 20시 42분
주민등록번호 노출건수	6 건
위험도	상

패턴 분석 및 주민등록번호 유효성 검사를 통하여 [사이트명]에 노출된 주민등록번호가 있는지 진단합니다. 주민등록번호는 개인정보의 가장 중요한 정보로써 노출 시 사이트에 별 적인 조치가 가능할 수 있습니다.

노출내용	1111012122021	노출건수	2 건
순번	URL 항목		
1	노출 URL : http://www.sde-s1.knoe		
재검색	상위 URL : http://www.ckboard.co		

3. 개인정보 침해사고 처분 기준

가. 관련

- 「개인정보보호법」 주요 내용 및 개인정보 침해사고 처분 강화 안내
(정보직업교육과-5475, 2011. 3. 25.)

나. 추진배경

- 개인정보 유출 통지, 벌칙 강화 등 기존보다 확대·강화된 「개인정보보호법」 시행에 따라 개인정보 노출을 포함한 개인정보 침해사고에 대해 2009.12월에 안내한 기준에 따라 처분을 강화함

※ 우리교육청 '개인정보 노출 진단시스템'의 진단결과도 처분대상임

다. 처분기준

- 처분대상자의 고의, 과실 및 비위정도, 대상정보의 민감·중요 정도 등을 종합적으로 판단하여 처분

비위의 유형 \ 비위의 정도 및 과실	비위의 도가 무겁고 고의가 있는 경우	비위의 도가 무겁고 중과실이거나 비위의 도가 가볍고 고의가 있는 경우	비위의 도가 무겁고 경과실이거나 비위의 도가 가볍고 중과실인 경우	비위의 도가 가볍고 경과실인 경우
5. 비밀엄수의무 위반				
가. 비밀의 누설·유출	파면	파면-해임	강등-정직	감봉-견책
나. 비밀분실 또는 해킹 등에 의한 비밀침해 및 비밀유기 또는 무단 방치	파면-해임	강등-정직	정직-감봉	감봉-견책
다. <u>개인정보 부정이용 및 무단 유출</u>	파면-해임	해임-강등	정직	감봉-견책
라. <u>개인정보 무단조회·열람 및 관리 소홀 등</u>	파면-해임	강등-정직	감봉	견책
마. 그 밖의 보안관계 법령 위반	파면-해임	강등-정직	감봉	견책

※ 교육공무원 징계양정 등에 관한 규칙(별표. 징계양정기준, 2011. 7. 18.)

※ 인천광역시교육감 소속 지방공무원 징계양정에 관한 규칙
(별표1. 징계양정기준, 2011. 12. 12.)

4. 개인정보업무 필수 이행사항

가. 관련

- 중·고교 학생증 발급관련 개선에 대한 심의·의결 결과 송부
(개인정보보호위원회 심의처리과-456, 2012.11.28.)
- 개인정보 처리실태 개선 협조 요청(정보지원과-2233, 2013.2.22.)
- 공공기관의 개인정보 목적외 이용·제공 및 열람 처리시 유의 사항 알림
(정보지원과-4715, 2013.3.22.)

나. 무분별한 개인정보 수집 제한

- 목적달성에 불필요한 주민등록번호 등 개인정보 수집 제한

다. 주민등록번호 등 고유식별정보와 종교, 건강정보 등 민감정보 원칙적 처리 금지

- 고유식별정보(주민등록번호, 여권번호, 운전면허등록 번호)는
 - ① 정보주체의 별도의 동의
 - ② 법령에서 구체적으로 명시하거나 허용하는 경우를 제외하고는 처리할 수 없음

라. 개인정보 위탁시 또는 목적외 이용이나 제3자 제공에 대한 주의

- 개인정보 위탁 관련 업무는 반드시 법령이 정한 바에 따라 준수
- 법령에 근거 없이 개인정보를 수집목적과 다르게 이용하거나, 제3자에게 제공하지 않도록 주의, 인터넷에 잘못 게시하여 개인정보가 유출되는 경우도 불법적인 제3자 제공으로 처벌 받을 수 있음

마. 개인정보파일은 DB보안 프로그램, 암호화 소프트웨어 등 안전한 방법으로 보관

바. 이미 수집된 개인정보파일을 이용한 후에는 알아볼 수 없도록 파기

- 개인정보의 보유 이용기간이 끝난 경우 또는 이용목적을 달성한 경우에는 문서를 분쇄하거나 소각해 파기해야 하며, 컴퓨터로 저장된 문서의 경우 포맷이나 삭제 소프트웨어 사용하여 파기

사. 관련 문서를 명확히 구비하고 정보주체의 열람청구에 신속히 대응

- 개인정보처리방침, CCTV 안내판, CCTV 운영방침 등 의무적 공개가 필요한 문서들과 내부관리계획(개인정보보호 추진계획)등 수립하여야 하는 문서를 점검하여 누락되지 않도록 준비
- 정보주체의 열람청구 등에 대한 정보주체의 요구가 있을 경우 지체 없이 처리

아. 개인정보보호 위한 기술적 의무 이행사항

- SSL 보안서버 구축
 - 대상 : 개인정보보유시스템
 - 구축기한 : 2012.3.31.까지
- 표준보안 API
 - 대상 : 전자서명을 통한 업무담당자의 본인확인이 필요한 시스템
 - 구축기한 : 2012.6.30.까지
- DB 암호화
 - 대상 : 고유식별정보, 비밀번호, 바이오정보 저장 시스템
 - ※ 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
 - 구축기한 : 2012.12.31.까지
- I-PIN 적용
 - 대상 : 회원가입시 주민등록번호를 수집하거나 게시판 본인 확인시 주민등록번호 사용 기관
 - 구축기한 : 2012.3.31까지

▣ 업무별 문의처 안내 ▣

담당업무	담당자	연락처	전자우편	비 고
정보보호팀 업무 총괄	유창호	420-8441	ykjw6372@ice.go.kr	
정보보안 총괄, 교육종합정보망 관리	진교권	420-8488	eubi40@ice.go.kr	
개인정보보호, 학교통합홈페이지 구축	송영의	420-8488	edukings@ice.go.kr	
네트워크 보안시스템 관리, 정보시스템 보안성 검토	이경미	420-8234	hitech96@ice.go.kr	
홈페이지 보안 관련 업무, 정보공유및침해대응시스템 운영	김형열	420-8234	hykim@ice.go.kr	
PC통합보안시스템, 사이버보안 진단의 날 운영	윤석민	420-8244	dubu76@ice.go.kr	
NXG200GX 운영 지원	전영익	426-3600	-	상주 직원
망(회선)관리	이세왕	426-3600	-	
통합관제시스템 운영 지원	김용찬	420-8428	-	
웹방화벽 운영 지원	김성수	420-8428	-	
PC통합보안시스템 운영 지원	최득용	420-8428	-	