용역사업 보안 가이드라인

사 업 명	데이터베이스 구축(3단계)
주관기관	뉴딜코리아

2015. 11

뉴딜코리아
정보보호컨설팅

담당	컨설팅	팀장 서재균	Tel 02) 3410-4031
	컨설팅	차장 백동수	Fax

- 목 차 -

[붙임3] 용역사업 보안 가이드라인

용역사업 보안 가이드라인

o [별표1] '정보보안 특수계약조건'이 계약서에 포함된다.

o 사업자는 ABC기관「**정보보안업무 규정**」을 준수해야 한다.

o 사업자는 보안담당자를 지정하고 [**별표4**]의 '**사업자 보안관리 준수사항**'을 이행해야 한다.

o 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 **[별표2]**의 **'누출금지 대상정보'**에 대한 보안관리계획을 사업제안서에 기재하여야 하며, 해당정보 누출 시 사업자는 국가법계약법 시행령 제76조에 따라 사업자를 부정당업체에 등록한다.

o 사업자는 사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행 중은 물론 사업 완료 후에도 이를 외부에 유출해서는 안되며, 사업 종료시 정보보안담당자의 입회하에 완전 폐기 또는 반납해야 한다.

o 사업자는 「개인정보보호법」제33조에 따라 개인정보 영향평가가 필요한 경우에는 영향평가팀에 참여하여 제반 업무를 지원해야 한다.

o 사업자는 사업 최종 산출물에 대해 정보보안전문가 또는 전문보안 점검 도구를 활용하여 보안 취약점을 점검, 도출된 취약점에 대한 개선을 완료하고 그 결과를 제출하여야 한다. 웹 기반 서비스의 경우에는 실제 서비스 전에 보안전문가를 통한 모의해킹을 실시하고, 도출된 취약점을 개선해야 한다.

[별표1] 정보보안 특수계약조건

정보보안 특수계약조건

제1조(정보누출 등 금지행위) "사업자"는 본 사업을 수행함에 있어 다음 각 호의 행위를 하여서는 아니 된다.

1. 별표 2에 명시된 누출금지 대상정보를 누출하는 행위
2. 별표 3에 명시된 보안위반 처리기준의 금지행위

제2조(벌칙) ①"사업자" 또는 "사업자"의 대리인·지배인, 그 밖의 사용인이 제1조제2호의 금지행위를 한 경우에는 별표 3의 보안위반 처리기준에 명시된 벌칙을 "사업자"에게 적용한다.

② 제1항에 따른 위약금 부과는 유지보수료 청구 시 해당하는 금액만큼 삭감한다.

③ 제1항에 따른 관계자 행정조치는「공무원징계령」에 따라 조치한다.

제3조(하도급 계약시 조치사항) "사업자"가 본 사업을 수행하기 위하여 하도급 계약을 체결할 경우에는 본 사업계약 수준의 정보보안 특수계약조건을 하도급계약서에 포함하여야 한다.

[별표2] 누출금지 대상정보

누출금지 대상정보

보호등급	대상정보
<가 등급> 비밀 및 대외비급 비공개 대상 정보	①「공공기관의 정보공개에 관한 법률」제9조제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서 ②「개인정보보호법」제2조제1호의 개인정보 ③「보안업무규정」제4조의 비밀 및 동 시행규칙 제7조제3항의 대외비 ④ 그 밖에 각급기관의 장이 공개가 불가하다고 판단한 자료
<나 등급> 정보시스템 관련 중요 정보	① 정보시스템의 내·외부 IP주소 정보 ② 정보시스템 세부 구성에 관한 정보 - 세부 정보시스템 구성현황 및 정보통신망 구성도 - 국가용 보안시스템 및 정보보호시스템 도입 현황 - 침입차단시스템·방지시스템 등 정보보호제품 설정 정보 - 라우터·스위치 등 네트워크 장비 설정 정보 ③ 정보통신망 취약점 분석·평가 결과물 ④ 사용자계정·비밀번호 등 정보시스템 접근통제 정보
<다 등급> 용역결과물 및 기관 내부 문서	① 반출승인을 받지 않은 용역사업 결과물 또는 프로그램 소스코드 ② 외부 공개대상이 아닌 기관 내부 문서

[별표3] 보안위반 처리기준

보안위반 처리기준

구분	위규사항	처리기준
심각	1. 누출금지 대상정보 '가' 급 정보에 대한 유출 및 유출 시도 가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 유출 나. 개인정보·신상정보 목록 유출 다. 비공개 항공사진·공간정보 등 비공개 정보 유출 2. 정보시스템에 대한 불법적 행위 가. 관련 시스템에 대한 해킹 및 해킹시도 나. 시스템 구축 결과물에 대한 외부 유출 다. 시스템 내 인위적인 악성코드 유포	▪ 사업참여 제한 ▪ 재발 방지를 위한 조치계획 제출 ▪ 관계자 행정조치 ▪ 위반자 대상 특별보안교육 실시
중대	1. 누출금지 대상정보 '가'급과 '나' 급 정보에 대한 관리소홀 가. 시건되지 않은 장소 및 노출된 장소에 관리자 없이 방치 나. 휴지통·폐지함 등에 유기 또는 이면지 활용 다. 개인정보·신상정보 목록을 책상 위 등에 방치 라. 기타 비공개 정보에 대한 관리소홀 2. 사무실·보호구역 보안관리 허술 가. 통제구역 출입문을 개방한 채 퇴근 등 나. 인가되지 않은 작업자의 내부 시스템 접근 다. 통제구역 내 장비·시설 등 무단 사진촬영 3. 전산정보 보호대책 부실 가. 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 나. 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 다. 개발·유지보수 시 원격작업 사용 라. 저장된 비공개 정보 패스워드 미부여 마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장 바. 외부용 PC를 업무망에 무단 연결 사용 사. 보안관련 프로그램 강제 삭제 아. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)	▪ 위반시 위약금 부과 (500만원 이하) ▪ 관계자 행정조치 ▪ 재발 방지를 위한 조치계획 제출 ▪ 위반자 대상 특별보안교육 실시

보통	1. 누출금지 대상정보 '나' 급 정보에 대한 관리소홀 가. 주요 현안·보고자료를 책상위 등에 방치 나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용 2. 사무실 보안관리 부실 가. 캐비넷·서류함·책상 등을 개방한 채 퇴근 나. 출입키를 책상위 등에 방치 3. 보호구역 관리 소홀 가. 통제·제한구역 출입문을 개방한 채 근무 나. 보호구역내 비인가자 출입허용 등 통제 미실시 4. 전산정보 보호대책 부실 가. 휴대용저장매체를 서랍·책상 위 등에 방치한 채 퇴근 나. 네이트온 등 비인가 메신저 무단 사용 다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅·화면보호 패스워드 미부여 또는 "1111" 등 단순숫자 부여 마. PC 비밀번호를 모니터옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	▪ 위반시 위약금 부과 (300만원 이하) ▪ 관계자 행정조치 ▪ 재발 방지를 위한 조치계획 제출 ▪ 위반자 대상 특별보안교육 실시
경미	1. 누출금지 대상정보 '다' 급 정보 및 업무관련서류 관리 소홀 가. 시건되지 않은 장소 및 노출된 장소에 관리자 없이 방치 나. 않은 저장매체 또는 인터넷 연결 단말기에 보관 다. 권한이 없는 사용자가 보관 2. 사무실 보안관리 소홀 가. 근무자 부재시 출입문을 개방상태로 방치 또는 출입문 열쇠 방치 나. 각종 보안장비 운용 미숙 및 경보·보안장치 작동 불량 3. 전산정보 보안대책 부실 가. 보안 소프트웨어(백신, 내 PC 지키미 등) 주기적 점검 미실시 나. 인터넷 웹하드·P2P 등 인터넷 자료공유사이트 이용 다. PC 부팅·윈도우 비밀번호 미설정 또는 노출 라. 보조기억매체 방치 마. PC내 보안성이 검증되지 않은 프로그램 사용	▪ 월2회이상 위반 시 위약금 부과(100만원 이하)

[별표4] 사업자 보안관리 준수사항

(1) 참여인원에 대한 보안관리

- o 인원투입시 ABC기관 보안관리 사항에 대한 기본 보안교육을 수행하고, '보안서약서' 및 '기본보안교육 확인서'를 담당공무원에게 제출한다.
- o 인원 투입 종료시 '비밀누설금지 서약서'를 담당공무원에게 제출 한다.
- o 인원변동 현황 및 각종 서약서 징구여부를 '인원관리대장'을 통하여 관리 보관한다.
- o 용역업체 참여인원은 용역업체 임의로 교체할 수 없으며 신상변동(해외여행 포함) 사항발생시 ABC기관에 즉시 보고한다.

(2) 자료에 대한 보안관리

- o ABC기관으로부터 제공받거나 자체 생산한 산출물 중 별표 2의 누출금지 대상정보 중 '가'급과 '나'급에 해당하는 자료(이하 "비밀자료"라 한다.)에 대해서는 자료의 인수·인계시 '자료관리 대장'을 작성하여 관리하고, 사업완료시 관련자료를 반납·파기한다.
- o 사업과정에서 생산된 모든 산출물은 ABC기관에서 제공하는 파일서버나 ABC기관 보안관리자가 지정한 단말기에 저장·관리한다.
- o 사업 관련자료는 인터넷 웹하드·P2P 등 인터넷 자료공유사이트 및 개인 메일함에 저장을 금지하고 ABC기관과 사업자간 이메일을 이용해 자료전송이 필요한 경우에는 자체 기관메일을 이용, 첨부자료 암호화 후 수·발신해야한다.
  단, 비밀자료는 전자우편으로 수·발신을 금지한다.
- o 상용이메일의 사용을 금지하며, 자체 기관메일 사용이 필요한 경우 ABC기관 정보보호 관리자의 승인을 받고 사용해야 한다.
- o 비밀자료는 지정된 사용자만 접근이 가능하도록하고 다른 정보와 구분하여 보관하여야 하며, 비밀자료를 제외한 일반자료는 사무실내 시건장치가 된 보관함에 보관한다.

(2) 사무실·장비에 대한 보안 관리

- o ABC기관 사무실 사용시 출입문이 상시 개방되지 않도록 시건장치를 관리하고, 외부 사무실 사용시 CCTV·시건장치 등 비인가자 출입통제 대책을 마련한다.
- o 사무실 출입문의 열쇠·출입증 등을 분실 또는 접근통제 장치의 이상이 발생한 경우에는 24시간내 ABC기관에 보고하고, 48시간내 교체 또는 수리한다.
- o 일일 당직근무자를 지정하여 퇴근전 문서 및 USB 방치 점검 등 일일 보안점검을 수행한다.
- o 사업수행시 단말기의 반입시 악성코드 감염여부 및 최신 백신업데이트 확인, 보안점검을 수행해야 하며, 반출시 모든 데이터는 완전삭제 조치한다.
- o 인가받지 않은 USB메모리 등의 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 ABC기관의 승인하에 사용한다.
- o 업무용 단말기내 보안USB 통제 프로그램을 설치해야하고, 임의적인 단말기 해체를 방지하기 위한 봉인지가 훼손되지 않도록 관리하며, USB사용 및 봉인지 해제시 ABC기관의 사전승인을 받아야 한다.

(3) 내·외부망 접근시 보안관리

- o 사업자는 승인받은 장비에 대하여 부여된 권한·목적에 대해 승인받은 기간(최대1년)동안 사용하고, 사용이 종료된 시점에 즉시 반납한다.
- o 인터넷 연결 단말기는 검색용도로만 사용해야하며, 해당 단말기내 사업관련 자료의 보관을 금지한다.
- o 사전 승인없이 ABC기관 네트워크에 무단 연결을 금지한다.

(4) 보안점검 및 교육

- o 사업자는 보안인식제고를 위해 월1회 자체 보안 교육을 하고, ABC기관이 요구하는 보안교육에 참석한다.
- o 사업자는 사무실 또는 업무를 수행하는 공간에 대해 일일 보안점검을 하고, 월1회 자체 보안점검을 실시한다.
- o 상기 보안교육 및 보안점검 결과, 인원 및 전산장비 변동사항, 보안이슈에 대해 월 보안점검 및 결과보고서를 작성하여 ABC기관에 제출한다.

※ 상기 사업자 보안관리 준수사항 중 예외적 허용이 필요한 경우에는, ABC기관 정보보안담당에게 예외 허용사항에 대한 보안성 검토를 요청한다.