등록번호	전산정보과-6006
등록일자	2015.5.20.
결재일자	2015.5.20.
공개구분	부분공개

주무관	전산운영팀장	전산정보과장	주민자치국장
박수진	황금영	서용선	05/20 이경헌
협 조	정보통신팀장 심화성		

새올행정정보시스템 외부사용자 계정부여

보 안 관 리 추 진 계 획

서 대 문 구

전 산 정 보 과

새올행정정보시스템 외부사용자 계정부여

보 안 관 리 추 진 계 획

새올행정정보시스템 외부사용자 계정부여에 따른 보안관리 계획을 수립하여 정보시스템의 자료유출을 미연에 방지하고 안전한 시스템 관리에 철저를 기하고자 함.

Ⅰ 추진배경 관련규정

- ▢ 기간제 근로자 등의 외부사용자 계정 요청으로 새올행정정보시스템 접근 가능
- ▢ 원활한 업무수행을 위해 외부사용자의 최소한의 사용자 계정부여 불가피 (최소한의 권한 부여)
- ▢ 사용자 계정에 대한 중복사용 금지 등 보안기능 강화 필요
- ▢ 관련법 및 규정

명 칭	조 항	내 용
정보통신보안업무 규정(2000.12.)	제 27조(사용자계정관리)	· 신규 : 신청서 및 신원확인 · 퇴직 : 즉시 삭제 · 외부사용자 : 불허하되, 부득이한 경우 행정기관장의 책임하에 유효기간 설정, 보안조치 후 허용 · 장시간 미사용 계정 : 삭제
	제 47조(업무대행자 보안관리)	· 부득이한 경우 분임보안담당관 승인하에 보안 조치수행 후 업무대행자 지정(청원경찰, 일용직, 단순고용직, 공익근무요원 등)
행정기관정보시스템 접근권한 관리규정	제 12조(접근권한 부여원칙) 제 14조(접근권한 신청) 제 16조(이용자정보관리)	· 접근권한은 허용된 자에 한해 최소한으로 부여 · 권한관리책임자에게 접근권한 문서로 신청 · 권한관리책임자는 이용자 등록내역을 주기적으로 점검하여 부적절 이용자의 접근권한 삭제
개인정보보호법	제 60조(비밀유지 등) 제 72조(벌칙)	· 직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도 이용 불가 · 3년 이하의 징역 또는 3천원만 이하의 벌금

Ⅱ 비정규직 계정현황

☐ 대상시스템 : 새올행정정보시스템

☐ 외부사용자 계정부여 현황

사용부서	계정부여	권한범위	사용기간 (기본 설정값)	비 고
행정지원과	1명	일반공무원[1]	9999-12-31	공동계정
일자리경제과	1명	일반공무원	9999-12-31	개별계정
복지정책과	5명	일반공무원, 공직윤리사용자, 청탁일반사용자	9999-12-31	개별계정
사회복지과	2명	일반공무원, 서비스상담담당자, 후원담당자, 공직윤리사용자, 청탁일반사용자	9999-12-31	개별계정
여성가족과	1명	일반공무원, 업무처리담당자 접수 및 처리담당자, 공직윤리사용자, 청탁일반사용자	9999-12-31	개별계정
교통관리과	2명	일반공무원, 공직윤리사용자, 청탁일반사용자	9999-12-31	개별계정
의 약 과	4명	일반공무원	9999-12-31	개별계정
북아현동	1명	일반공무원	9999-12-31	개별계정
합 계	17명			

Ⅲ 보안관리 세부추진계획

☐ 시스템 접근에 대한 관리감독 강화

○ 외부사용자의 정보시스템 접근을 위한 사용자계정 부여는 원칙적으로 금지, 부득이한 경우 부서장 책임하에 허용

1) 일반공무원 : 일반 공무원과 같은 권한을 부여받을 수 있음. 일반사용자 권한 : 새올포털 메인 포틀릿 화면만 볼 수 있는 권한으로 업무적으로 사용불가

○ 계정 부여에 따른 조치사항

작업구분별 조치사항	① 개별 계정일 경우	② 공동 계정일 경우
계정요청	· 일반사용자 또는 일반공무원 권한인지 판단 후 권한부여 요청	
	· 추가적으로 부여받는 권한에 대해 상시 모니터링 실시 · 사용기간의 기본값(9999년 12월 31일)을 실제 사용기간으로 변경하여 설정	· 패스워드 3개월 기준으로 초기화(a12345) 하여 비밀번호를 수동으로 변경 · 사용기간을 1년 단위로 갱신하며 1년을 초과할 경우 보안서약서(부서장 및 부서별 담당자) 재징구
계정등록	· 사용자 계정 관리대장 관리 · 외부 사용자 정보 이용내역 상시 지도·감독 · 정보시스템에 불법 접속하는지 주기적으로 확인 · 작업이력에 대한 수시점검 실시	
기간만료	· 사용자 계정 회수 및 삭제 등 프로그램 설정(부서별 기간만료시 즉시 통보)	

▢ 사용자에 대한 계정부여 보안 방안

○ ① 개별 계정일 경우

- 요청부서장의 서명이 포함된 보안서약서 제출
- 당초 행정자치부 보안지침에서는 보안서약 및 신원조사를 필한 사용자에게 계정을 부여토록 하였으나 신원조사 기관(서대문경찰서)에서 비정규직에 대한 신원조사 불가통보로 보안서약서만 징구하며 이에 부서장 책임하에 주기적 보안교육 등을 실시
- 부서별 담당자 지정하여 통보
- 외부 사용자 계정부여 절차

① 부서장 책임하에 보안서약서 작성(부서장 서명포함, 요청부서) ② 사용자 계정 등록요청(요청부서) ③ 사용자 계정 추가 등록(전산정보과) ④ 접속주소, 접속시간, 접속사유 등 확인(전산정보과) ⑤ 업무권한 소멸시 즉시 사용자 계정 해지요청(요청부서) ⑥ 사용자 계정 회수 및 삭제(전산정보과)

○ ② 공동 계정일 경우

- 1년 단위로 부서장 및 담당자 서명 후 보안서약서 제출
- 관련부서 담당자 지정 통보

▢ 사용자 PC 등 보안 방안

○ USB 등 보조기억 매체의 반출입 제한

○ 업무용 PC는 원칙적으로 인터넷에 연결금지, 업무용으로만 사용

- 다만, 필요한 경우 보안책임자의 승인하에 방화벽 또는 인터넷 차단 S/W를 통해 필요한 사이트만 접속토록 통제

○ 기타 백신프로그램 설치, 시스템 암호 설정 등 기본적 보안조치

○ 업무관련 자료는 개인 PC, 메일함에 보관금지

○ 직무상 알게 된 개인정보는 누설금지(개인정보보호법 제 60조 비밀유지)

▢ 기타 보안 방안

○ 계정사용에 대한 로그 접속현황 관리 및 수시점검

○ 사용자 계정 오남용 예방을 위한 현장 방문 실사

Ⅳ 행정사항

▢ 계정 요청부서 협조사항

○ 부서장 책임(부서장 서명포함)하에 보안서약서 및 계정요청

- 공동 계정 요청부서는 1년 단위로 보안서약서 제출

○ 계정요청시 일반사용자 권한 또는 공무원 권한여부에 대한 정확한 권한요청 및 부서별 담당자를 지정하여 통보

○ 추가적인 권한부여는 요청부서에서 부여할 수 있는바 이에 신중한 권한부여 및 사용기간 최소한으로 재설정

○ 직무상 알게 된 개인정보에 대한 비밀유지 등 주기적 보안교육 실시

○ 기간만료시 계정 삭제요청

붙임 : 1. 정보통신보안업무규정 관련내용(27조, 47조) 1부.

2. 행정기관 정보시스템 접근권한 관리규정 관련내용(12조, 14조, 16조) 1부.

3. 개인정보보호법 관련내용(60조, 72조) 1부.

4. 보안서약서(양식) 1부.

[첨부 1]

❑ 정보통신보안업무규정(행안부 훈령 제147호, 2009. 6. 9.)

구 분	세부내용
제 27조 (사용자계정 관리)	① 시스템관리자는 사용자계정(ID)의 비인가자 도용 및 정보시스템 불법접속 등을 방지하기 위해 다음 각호 사항을 반영관리하여야 한다. 1. 신규 사용자계정 생성 시 신청서 작성, 신원확인 등의 절차로 발급 2. 퇴직, 보직변경 등으로 사용자계정을 해지해야할 때에는 신속히 삭제 3. 사용자계정을 공동으로 사용 금지 4. **외부 사용자의 계정부여는 불허하되, 부득이한 경우 행정기관장의 책임 하에 유효기간을 설정하는 등 보안조치를 강구한 후 허용** 5. 사용자 식별·인증 수단이 없는 사용자계정은 사용 금지 6. 휴면계정을 점검하여 필요하지 않은 경우 삭제 7. 계정을 주기적(사용자계정 6개월, 관리자계정 3개월)으로 점검하여 접근권한을 재검토하고 권한 남용을 감시
제47조 (업무대행자 보안관리)	① 행정기관의 장은 정보시스템을 관리하기 위하여 일용직, 단순고용직, 청원경찰, 공익근무요원 등을 업무대행자로 지정하여서는 아니 된다. 다만, **부득이한 경우에는 "시행요강 제3조제3항"에 의거 지정된 분임보안담당관의 승인 하에 지정**하되, 다음 각 호의 사항을 준수하여야 한다. **1. 정보시스템의 접속시간, 접속 및 이용 권한을 최소화** **2. 유효기간이 설정된 임시 접속계정 부여** **3. 비인가 정보시스템에 불법 접속하는지 여부를 주기적으로 확인 점검** ② 행정기관의 장이 제1항에 의하여 특정 정보시스템에 대해 업무대행자를 지정한 경우에는 다음 각호의 사항을 확인하는 등 보안조치를 수행하여야 하며, 그 사유가 소멸할 경우에는 즉시 해지하여야 한다. 1. 접속할 사용자, 사용자계정, 비밀번호 2. **접속주소, 접속시간, 접속사유(자료입력, 통계작성 등)** 3. 접속 종료 후 사용자계정 및 비밀번호 회수 등 조치사항

[첨부 2]

❑ 행정기관 정보시스템 접근권한 관리규정(총리훈령 제526호, 2008. 10. 29.)

구 분	세부내용
제 12조 (접근권한 부여원칙)	① 정보시스템 접근, 행정정보 열람 등 모든 접근권한은 법령 또는 업무 규정 등에 따라 **허용된 자에 한하여 업무수행에 필요한 최소한의 범위로 부여**하여야 한다. ② **접근권한을 부여받은 이용자는 접근권한을 임의로 양도, 대여해서는 안되며, 권한관리책임자는 이를 수시로 확인 및 지도·감독**하여야 한다.
제14조 (접근권한 신청)	① 정보시스템 또는 행정정보를 이용하고자 하는 **업무담당자, 시스템 관리자 및 외주 직원 등은** 신청서를 작성하여 부서장(외주 직원 등은 관할 부서장)의 결재를 받은 후 **권한관리책임자에게 접근권한을 신청**하여야 한다. 1. 정보시스템 행정정보의 이용 또는 활용 목적 및 근거 2. 이용 또는 활용하고자 하는 정보시스템 행정정보의 범위
제16조 (이용자 정보관리)	① **권한관리책임자는 이용자 등록 내역을 주기적으로 점검**하여 부적절한 이용자의 접근권한을 삭제하는 등 필요한 조치를 하여야 한다. ② **이용자는 정보시스템 또는 행정정보에 접근할 때 사용되는 행정전자서명인증서, 사용자계정(ID) 등 이용자 본인확인에 필요한 정보를 타인과 공유하지 않고 안전하게 관리**하여야 한다.

[첨부 3]

❑ 개인정보보호법(2014. 11. 19.)

구 분	세부내용
제 60조 (비밀유지 등)	다음 각 호의 업무에 종사하거나 종사하였던 자는 **직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도**로 이용하여서는 아니 된다.
제72조 (벌칙)	다음 각 호의 어느 하나에 해당하는 자는 **3년 이하의 징역 또는 3천만원 이하의 벌금**에 처한다. 3. 제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자