반송분석정보 정보보안 및 개인정보보호 지침

2012.09.30. 반송분석정보 제 2호

1.목적

이 지침은 제정 2012.2.3. 우정사업본부 훈령 제365호에 의거, 반송분석정보 정보보안활동에 필요한 세부사항 규정 및 반송정보센터에서 처리하는 개인정보를 보호하기 위하여 필요한 구체적 사항의 정함을 목적으로 한다.

2. 적용

이 지침은 반송분석정보 전산센터 및 각 지역 반송센터 등(이하 “센터”라 한다)에 대하여 적용한다.

3. 기본목표

반송분석정보 정보보안의 기본목표는 각종 전자적 수단에 의한 반송분석정보의 기밀성·무결성·가용성을 확보하고 반송분석정보 정보통신망을 보호하는 데 있다.

4. 기본활동 정보보안 담당자는 정보보안을 위하여 다음 각 호의 기본활동을 수행한다.

1. 정보보안 정책 및 활동 세부계획 수립·시행
8. 침해사고 대응·복구
9. 정보보안수준 평가·관리
10. 정보보안 교육계획 수립
11. 정보보안업무 심사분석
12. 도청 위해(危害)요소 제
13. 정보보안 관련 규정·지
14. 기타 정보보안 관련 사

5. 정보보안담당자 운영

① 정보보안업무를 수행하기

② ‘정보보안담당자’를 임명

연락처(전자우편 주소 포함

③ 정보보안담당자는 안전한

보안 기본활동을 수행한다.

6. 정보보안 정책 및 활동 세

정보보안담당자는 매년 정보

하고 우정사업 반송정보 담

7. 정보보안 감사·지도점검

① 각 센터 담당자는 매월

점검을 위한 정보보안일지를

② 정보보안담당자는 분기

9. 정보보안 교육

① 정보보안담당자는 센터 담당자 및 용역직원에 대해서 자체 연 1회 이상 정보보안 교육계획을 수립·시행한다.

② 정보통신시설의 보호를 위한 교육이 필요하다고 판단되거나 신규 직원이 전입 시에는 교육·훈련을 실시한다.

10. 인적 보안관리

① 반송정보분석장비 사용과 관련하여 사용자의 직위·임무별 작업 및 네트워크 접근 자격을 제안는 인적보안에 관련된 절차 및 방법을 마련한다.

② 반송정보분석 작업자에 대해서는 보안서약서 징구 등의 보안조치를 한다.

③ 사용자가 보직변경, 퇴직 등 인사이동이 있을 경우 관련 정보시스템 접근권한을 조정한다.

④ 외부 인력을 활용하여 정보시스템의 개발, 운용, 정비 등을 수행할 경우에는 해당 인력의 고의 또는 실수로 인한 정보유출이나 파괴를 방지하기 위하여 별도의 보안조치를 수행한다.

11. 무선통신 보안관리

반송정보분석작업 및 반송정보분석서비스는 무선통신을 사용하지 않는 것을 원칙으로 한다.

12. 전산자료 보안관리

① 전산자료에 대한 유출이나 파괴 또는 변조 등에 대비하여 다음 각 호에

6. 예비(Back up)체계 수립

② 전산자료를 입력 저장하

번호를 부여 관리 한다.

13. 정보통신망 관련자료 관

다음 각 호의 자료를 대외비

1. 정보통신망 세부 구성현

2. 보안시스템 운용현황

3. 보안취약성 분석평가 결

4. 기타 보호할 필요가 있는

14. 정보시스템 보안관리

① 정보통신망의 효율적인

자(이하 '시스템관리자'라 한

② 시스템관리자는 각종 서

자에게 불필요한 서비스를

③ 시스템관리자는 보안도구

하여야 하며 시스템 접속 시

1. 서버 접속일시, 접속자 및

2. 전산자료 열람·출력 등에

④ 시스템관리자는 자동 수

하고 외부유출 방지를 위한

⑦ 사용자별 자료 접근범위는 서버에 등록하여 인가 여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제한다.

⑧ 정보시스템에 대하여 전문보안업체에 의뢰 시 작업을 허용하여서는 아니 된다. 다만, 부득이한 경우에는 필요한 보안대책을 강구한 후 정보보안담당관의 승인을 받아 허용할 수 있으며, 이때에도 원격 유지보수 내용을 확인 감독하여 반드시 기록으로 유지하여야 한다.

15. 재난복구 대책

① 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애(障碍) 발생에 대비하여 서버를 IDC센터에 설치하고 시스템을 이원화, 백업관리 및 복구 등 종합적인 재난복구 대책을 수립·시행 한다.

② 정보통신망 장애를 대비한 백업시설을 확보하고 매일 정기적으로 작동 백업을 수행한다.

16. PC 등 단말기 보안관리

① 사용자는 PC·노트북·PDA 등 단말기(이하 “PC 등”이라 한다) 사용과 관련한 일체의 보안관리 책임이 있다.

② 정보보안담당자는 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안 대책을 강구하고, 사용자는 이를 준수한다.

1. 장비(CMOS 비밀번호)·자료(문서자료 암호화 비밀번호)·사용자(로그온 비밀번호)별 비밀번호를 사용하고 월 1회 주기적으로 변경

를 의뢰하고자 할 경우에는
않도록 보안조치를 하여야 ㅎ

④ 보안관리자는 PC 등에
관리한다.

⑤ 개인소유의 PC(노트북 P
사용하여서는 아니 된다. 다
받아 보안조치 후 반입 또는

⑥ PC 사용자는 상용 무선
을 위한 장치를 임의로 설치

⑦ 백신관리, 문서보안관리,
PC보안 장치를 임의로 삭제

17. 사용자계정 관리

① 반송정보분석서비스의 사
불법접속에 대비하여 다음

1. 권한관리로 접근권한 부
2. 사용자 접근시 IP 주소를
3. 비밀번호가 없는 사용자
3회에 걸쳐 사용자인증 실

② 시스템관리자는 사용자의
사용자계정이 발생할 경우

② 비밀이나 중요자료에는 반드시 자료별 비밀번호를 부여하되 공개 또는 열람 자료에 대하여는 그러하지 아니할 수 있다.

③ 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고 분기 1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어는 사용을 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 말 것
5. 이미 사용된 비밀번호는 재사용하지 말 것
6. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

19. 악성코드 감염 방지대책

① 각급기관의 장은 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 아래와 같은 대책을 수립 시행한다.

1. 사용자는 개인PC에서 작성하는 문서·데이터베이스 작성기 등 응용프로그램을 보안패치하고 백신은 최신상태로 업데이트·상시 감시상태로 설정 및 주기적인 점검을 실시하여야 한다.
2. 사용자는 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지하고 인터넷 등 상용망으로 자료 입수 시 최신 백신으로 불법 다운로드 되지 않

② 악성코드 감염이 발견되 다음 각 호의 조치를 하여야

1. 악성코드 감염피해를 최 용 중지 및 내부망과 격
2. 최신 백신 등 악성코드
3. 악성코드의 감염확산 방 및 보안조치 사항을 즉

③ 각급기관의 정보보안담당 는 우정사업본부 정보보안담

④ 우정사업본부 정보보안담 권고할 경우 각급기관은 즉

20. 웹서버 등 공개서버 관리

① 외부인에게 공개할 목적 부망과 분리하여 운영하고 설치하는 등 보안대책을 강

② 서버에 접근할 수 있는 한다.

③ 홈페이지 게재내용은 해 지 않도록 하여야 한다.

⑦ 공개서버를 통해 개인정보가 유출, 위·변조되지 않도록 보안조치를 하여야 한다.

21. 웹서비스 보안성 검증

① 웹서비스 보안성 검증은 부내의 모든 웹서비스를 대상으로 하는 것을 원칙으로 한다.

② 웹서비스는 별도의 보안프로그램 모듈을 개발하여 보안의 안정성을 최우선한다.

③ 정보보안담당자은 웹서비스 보안성 검증을 거쳐 안전하다고 판단된 경우에만 해당 웹서비스를 허용한다.

④ 반송정보 다운로드 정보의 보안을 위하여 각 업체별 담당자의 개인 MAC 정보를 체크하여 등록된 정보와 동일한 PC로의 다운로드만 허가한다.

22. 사이버공격 초동조치

① 정보통신망에 대하여 해킹, 웜·바이러스 유포 등 사이버공격 인지 시 피해실태를 파악하고 관련 로그자료 보존 및 필요 시 전산망 분리 등 초동조치 한다.

② 사이버공격에 의한 피해시스템은 사고원인 규명 시까지 증거보전을 의무화하고 임의 자료삭제 또는 포맷을 하여서는 아니 된다.

23. 침해사고 대응조치

① 사용자는 전자적 침해사고의 징후가 있거나 전자적 침해사고의 발생을

복구조치를 신속히 한다.

25. 정보시스템 보안관제 관

① 정보보안관제는 기본적
를 받는 것을 기본으로 한
② 보안관제 소프트웨어 설
③ 시스템관리자는 해당 정
가 정상 동작하도록 한다.
④ 시스템관리자는 정보시
보안관제 소프트웨어의 작
전문업체에 통보한다.
⑤ 보안관제 에이전트의 작
로 재작동할 수 있도록 해
스템관리자는 적절한 조치를

26. 바이러스 방역 관리

① 신규 보급하는 모든 PC
도록 하고, PC 운영체제 재
시 설치하여 항상 정상 작
② 사용자는 백신프로그램을
를 점검하고 치료한다.

한다.

3. 개인정보관리의 책임관계를 명확히 한다.
4. 개인정보의 수집·이용 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 처리정보의 열람청구권 등 정보주체의 권리를 보장한다.

② 개인정보를 취급 및 관리하는 자는 제1항의 규정에 의한 개인정보보호 기본방침을 따르고 개인정보를 보호하기 위하여 적극 노력한다.

28. 개인정보보호책임자

① 개인정보보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보보호대책 수립에 관한 업무
2. 개인정보보호 조직체계 구축 및 운영에 관한 업무
3. 개인정보의 수집, 저장, 이용, 제공, 폐기 및 관리에 관한 총괄 업무
4. 개인정보에 관한 침해사고 예방 및 지원에 관한 업무
5. 업무종사자 또는 제3자에 의한 위법·부당한 개인정보 침해 행위에 대한 점검
6. 서비스이용자로부터 제기되는 개인정보에 관한 불만이나 의견의 처리 및 감독
7. 개인정보보호 교육, 이행점검, 모니터링, 침해행위, 불만·의견 처리 등에 관한 사항
8. 기타 개인정보보호를 위하여 우정사업본부장이 지시하는 업무 및 서비스이용자의 개인정보 보호에 필요한 사항

방침"이라는 명칭을 사용하
사항과 구분

30. 개인정보 접근권한 부여

개인정보에 접근할 수 있는
고 각 업무 담당자별로 개
등하여 부여한다. 또한 접근
내용은 별도 기록을 유지하

31. 개인정보의 비밀유지

서비스의 제공을 위하여 개
무상 알게 된 개인정보를 제

1. 내부직원 : 업무상 알게
   교육을 통해 주지시키고
2. 외부직원 : 외부업체에게
   유출시 책임사항에 대해

32. 회원탈퇴 및 동의의 철회

정보주체가 인터넷 홈페이
인정보처리자가 제공하는 서
는 제공에 대한 동의를 철
인되면 지체 없이 해당 정
보를 파기해야 한다.

1. 전자매체에 수록된 개인정보(파일, 전자문서 등) : 파일의 복구기술이 발달되고 있는 점을 감안하여, 파일 삭제 및 파기시 철저한 덮어쓰기 등 재생이 불가능 하도록 기술적 방법을 사용하여 조치한다.
2. 출력물로 나타난 개인정보(우편물 등) : 각 센터에서는 해당 집중국에 인계 후 우정사업본부의 파기원칙에 따라 파기시키는 것을 원칙으로 한다. 인계 시에는 인수인계의 절차에 따라 진행한다.

25. 개인정보의 안정성 확보 각급기관의 장은 개인정보를 처리함에 있어 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 조치를 강구하여야 한다. 이러한 조치 사항은 다음 각 호와 같다.

1. 개인정보처리시스템 및 취급 PC의 백신 프로그램 설치
2. 개인정보처리시스템 보호를 위한 침입차단, 탐지 시스템의 설치
3. 개인정보처리시스템에 대한 정기적인 취약성 진단 및 개선
4. 기타 개인정보의 안정성 확보를 위한 기술적·관리적 조치

26. 개인정보 침해대응

① 개인정보 침해사고의 징후 또는 개인정보 관련 보안사고가 발견되는 즉시 발견자는 개인정보보호책임자에게 신고하여 적시에 대응할 수 있도록 한다.

② 개인정보 침해사고에 대한 내용은 지정된 보고자 외에 다른 사람에게 유출해서는 아니 된다.

지한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할
   할 수 있는 방법 등에
4. 개인정보처리자의 대응
5. 정보주체에게 피해가 발
   및 연락처

28. 정보시스템 저장자료 삭

정보시스템 저장매체에 저

1. 정보시스템의 사용연한
2. 정보시스템 무상 보증
   보시스템을 교체할 경
3. 정보시스템의 임대기간
4. 고장 수리를 위한 외부
   를 보안 통제할 수 없
5. 기타 정보시스템 사용
   판단되는 경우

29. 정보시스템 도입시 보안

① 정보시스템의 도입시 고