스마트워크 활성화를 위한 정보보호 권고 (2011.1)

제1장 총칙

제1조(목적) 본 권고는 보안위협으로부터 스마트워크 이용자를 보호하고, 안전한 스마트워크 이용환경을 조성하기 위하여 서비스 제공 및 이용과 관련한 모든 기업들이 자율적으로 이행할 수 있는 기술적, 관리적 보호조치를 제시하고 이의 준수를 권고하는 것을 목적으로 한다.

제2조(정의) 본 권고에서 사용되는 용어의 정의는 다음과 같다.

1. “스마트워크”라 함은 「정보통신망이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제1호에 따른 정보통신망을 활용하여 언제, 어디서나 편리하게 효율적으로 업무에 종사할 수 있도록 하는 업무형태를 말한다.
2. “스마트워크 센터”라 함은 각 지역 주거지 인근에 구축된 전용 시설(센터)로 IT 인프라를 활용한 사무실과 유사한 근무 환경을 말한다.
3. “재택근무”라 함은 IT를 활용하여 자택에 업무공간을 확보하고 업무에 필요한 시설과 장비를 구축한 근무 환경을 말한다.
4. “모바일 오피스”라 함은 스마트폰, 스마트 패드, 노트북 등의 모바일 단말기를 이용하여 시간적, 공간적 제약 없이 업무를 수행하는 근무 환경을 말한다.
5. “영상 회의”라 함은 원거리에 위치한 사람들이 통신망을 통해 한 장소에 있는 것과 같이 진행하는 회의를 말한다.
6. “스마트워크 서비스 제공자(이하 서비스 제공자)”라 함은 스마트워크 서비스를 위한 인프라, 플랫폼 등을 구축하여 임대하는 기업 또는 조직을 말한다.
7. “스마트워크 관리자(이하 관리자)”라 함은 스마트워크 서비스를 도입한 기업 또는 조직의 스마트워크 관련 구성요소(단말기, 네트워크 등)의 관리 및 보안정책 수립, 운영 등의 업무를 수행하는 자를 말한다.
8. “스마트워크 이용자(이하 이용자)”라 함은 스마트워크 서비스를 이용하는 임직원을 말한다.
9. “중요정보”라 함은 기업의 영업활동에 중대한 영향을 미치는 기업기밀에 해당되는 정보를 말한다.

제3조(적용 대상 및 범위) 본 권고는 스마트워크 서비스 제공자, 관리자, 이용자를 적용 대상으로 한다.

제2장 스마트워크 서비스 제공자 준수사항

제4조(인프라 보안) 서비스 제공자는 안전하고 신뢰할 수 있는 스마트워크 인프라 환경을 조성하기 위해 다음과 같은 기술적 보호대책을 마련해야 한다.

1. 해킹대응 기술 : 서비스 제공자는 스마트워크 인프라 보호를 위해 악성코드 대응 및 유해트래픽 차단 등 악의적인 공격을 사전에 탐지하고 차단할 수 있어야 하며, 장애 발생 시 신속한 대응 및 복구를 통해 지속적인 스마트워크 서비스 제공이 가능하도록 조치해야 한다.
2. 유·무선 네트워크 보안 : 서비스 제공자는 유·무선 네트워크 및 기존의 레거시 시스템과의 연동구간에 대한 보안성과 가용성을 고려한 시스템을 구축하고, 무선 네트워크에 대한 단말기 인증과 암호화 통신 등의 보안기능을 제공해야 한다.
3. 물리적 보안 : 서비스 제공자는 비인가자의 스마트워크 센터 및 서비스 제공을 위한 주요 네트워크, DB, 서버 등 인프라 시설에 대한 접근을 통제할 수 있도록 CCTV, 바이오인증, 스마트카드 등 물리적 보안대책을 마련해야 한다.

제5조(공용 PC 보안) 서비스 제공자는 스마트워크 센터 내 공용 PC(이하 스마트워크용 PC)를 통한 중요정보 취급 시 다음과 같은 보안대책을 마련해야 한다.

1. 스마트워크용 PC의 자체 기억저장장치에 업무관련 정보는 PC 사용 후 저장되지 않도록 한다.
2. 스마트워크용 PC의 USB 포트 등 이동식 저장매체와의 연결 슬롯은 사내에 정의된 스마트워크 관리 규정(이하 내부 규정)에 따라 비활성화 할 수 있다.
3. 스마트워크용 PC의 접속 네트워크는 내부 규정에서 지정한 통신 수단만을 이용해야 한다.
4. 스마트워크용 PC에는 내부규정에 의해 허가된 소프트웨어만 설치해야한다.
5. 스마트워크용 PC를 사용하여 가상 데스크톱에 접속할 경우, 특정업무와 관련한 중요정보에 접근이 제한될 수 있다.

제3장 스마트워크 관리자 준수사항

제6조(단말기 보안) 관리자는 스마트워크 서비스에 이용되는 단말기를 통한 중요정보 취급 시 다음과 같은 관리적 보호대책을 반드시 적용해야 한다.

1. 단말기 보안 플랫폼 : 관리자는 단말기 내 중요정보가 유출되지 않도록 단말기 잠금 및 암호기능을 제공하고 웜·바이러스 등의 악성코드 감염에 대응하기

위한 모바일 전용 백신 설치, 보안패치 적용, 펌웨어 업데이트 등의 보호대책을 마련해야 한다.

2. 단말기 원격제어 : 관리자는 원격지에서 단말기에 대한 보안정책 설정 및 변경이 이루어질 수 있도록 원격제어 기능을 제공해야 한다.
3. 단말기 분실·도난 대비 : 관리자는 단말기 분실 및 도난에 의한 기업정보 또는 개인정보 유출에 대비하여 단말기 내 중요정보의 원격백업 및 삭제, 복원 등의 보호대책을 마련해야 한다.
4. 휴대 단말기 정보관리 : 관리자는 스마트워크 휴대단말기 내에 저장된 정보자산의 안전한 취급 및 관리를 위하여 다음과 같은 관리적 보안대책을 마련해야 한다.
   ① 휴대단말기에서 업무처리 시 중요한 정보는 암호화하여 저장해야 하며, 부득이한 경우 정보의 저장이 이루어지지 않도록 업무처리 종료 후 정보를 삭제해야 한다.
   ② 휴대단말기의 USB 포트 등 이동식 저장매체와의 연결 슬롯은 내부 규정에 따라 비활성화 할 수 있다.
   ③ 휴대단말기의 메모리슬롯 및 사람거리통신망(PAN : Personal Area Network) 이용은 내부규정에 의해 비활성화 될 수 있다.
   ④ 휴대단말기 네트워크 접속은 내부규정에서 지정한 통신수단만을 이용해야 한다.
   ⑤ 휴대단말기 내에는 내부규정에 의해 허가된 소프트웨어만 설치해야한다.
   ⑥ 관리자는 불가피한 경우 내부규정에 의해 휴대단말기를 통한 업무수행 영역을 제한할 수 있다.

제7조(서비스 보안) 관리자는 아래 각 호의 스마트워크 관련 서비스를 통해 중요정보 취급 시 다음과 같은 보안대책을 마련해야 한다.

1. 모바일 오피스 보안 : ① 모바일 오피스는 이용자와 단말기에 대한 복합인증을 제공해야 한다. ② 모바일 오피스의 기업정보 및 개인정보 등 중요정보는 VPN, 데이터 암호화 등의 통신보호 기능을 제공해야 한다. ③ 모바일 오피스의 중요정보는 송수신 시 단말기 내에 암호화하여 저장해야 한다.
2. 클라우드 서비스 보안 : ① 클라우드 서비스는 이용자의 식별 및 인증방식을 통합 관리해야 한다. ② 클라우드 서비스는 이용자의 개인화된 가상화 업무환경을 제공해야 한다. ③ 클라우스 서비스 내의 분산된 중요정보는 안전한 암호화 및 키 관리 등의 보호대책을 마련해야 한다.
3. 통합 커뮤니케이션 보안 : 사용자는 이메일, 그룹웨어, VoIP, 메신저 등의 통합 커뮤니케이션 내 비밀정보와 멀티미디어에 대하여 권한 없는 제 3자에 의한 수집 및 이용을 방지하도록 조치를 취해야 한다.
4. 영상회의 보안 : 사용자는 영상회의 멀티미디어에 대해서 권한 없는 제 3자에 의한 수집 및 이용을 방지하도록 영상정보에 노이즈 삽입 또는 암호화 등의

보안대책을 적용해야 한다.

5. 보안성 검증 : 사용자는 스마트워크 업무용 애플리케이션 아키텍처와 구현에 대한 보안성 검증을 수행해야 한다.

제8조(콘텐츠 보안) 관리자는 스마트워크 업무와 관련된 콘텐츠 보호를 위해 다음과 같은 보안대책을 적용해야 한다.

1. 암호화 : 사용자는 중요정보를 보호하기 위하여 이기종 단말기 간에 호환이 되는 DRM 및 데이터 암호화 등의 콘텐츠 보호 조치를 취해야 한다.
2. 정보자산의 분류 : 사용자는 스마트워크 서비스 도입을 위해 정보자산을 식별하고 중요도 기준에 따라 분류하여 정보자산 등급별 보호 조치를 취해야 한다.

제9조(인적자산의 관리) 관리자는 안전한 스마트워크 서비스 이용이 이루어질 수 있도록 이용자 대상의 관리적 보호대책들을 마련해야 한다.

1. 교육・훈련

① 스마트워크에 사용되는 장비 및 소프트웨어의 사용법에 대한 교육을 실시해야한다.

② 스마트워크와 관련한 정보보호 교육을 정기적으로 연 1회 이상 실시하여 스마트워크 정보보안 정책을 인식시켜야한다. 스마트워크 정보보호 교육의 내용은 다음 각 호와 같다.

가. 스마트워크 정보보호 기술이해 및 기술 사용법
나. 스마트워크 정보보호 내부규정 및 내부규정 미준수 시 벌칙 내용
다. 스마트워크 보안사고 발생 시 대응 방법
라. 스마트워크 업무 환경에 대한 안전조치 방법

2. 업무현황 모니터링

① 이용자들이 사용한 스마트워크용 PC, 휴대단말기는 기업정보 보호를 위해 내부 규정 준수 여부 및 사용현황을 모니터링할 수 있다.

② 관리자는 스마트워크 이용자들에게 업무현황 모니터링 여부를 사전에 알리고 동의를 받아야 한다.

③ 스마트워크 업무환경에 대해 다음 각 호를 준수여부를 점검한다.

가. 재택근무 및 스마트워크센터 이용 시 허가되지 않은 민감한 업무에 대한 정보의 접근 및 문서 등의 반출에 대한 점검
나. 휴대단말기 사용 시 업무수행 불가구역에서 내부 시스템 접근을 통한 업무수행 여부 점검
다. 재택근무 시 내부규정에 의해 분류된 기밀문서 등이 유출되지 않도록 안전

조치 등의 적용 여부

3. 조직 구성

① 관리자는 사내 정보보호 조직과 별도로 스마트워크를 위한 정보보안 관리 조직(스마트워크 정보보호 관리자 등)을 구성하거나, 기존의 조직 또는 관리자가 이를 겸임할 수 있다.

② 스마트워크 정보보호 관리자는 다음 각 호의 업무를 수행한다.

가. 사내 스마트워크 관리 규정을 총괄

나. 스마트워크관련 정보유출 및 침해사고 발생 시 이에 대한 대응을 총괄

다. 스마트워크 수행으로 인한 정보보호와 관련한 불만이나 의견처리 및 감독

라. 기타 스마트워크 정보보호를 위해 필요한 사항

마. 정보자산의 외부반출 시 이에 대한 인·허가와 관련한 기록

바. 이용자에 대한 정보보호 교육 계획 수립 및 이행

사. 스마트워크 내부규정이 제대로 이행되는지에 대한 점검 및 점검결과 기록

제10조(침해사고 대응절차 마련) 관리자는 스마트워크 환경에서 발생할 수 있는 다양한 보안 침해사고에 대한 대응절차를 마련해야 한다.

1. 단말기 분실 및 도난

① 스마트워크에 활용되는 PC 및 휴대단말기는 내부규정에 근거한 사용자 인증 절차에 따라 분실 및 도난 발생 시 제3자의 데이터 접근을 제한할 수 있어야 한다.

② 단말의 분실 및 도난 시 단말의 용도에 따라, 장치의 기능을 정지시키는 기능을 활성화하여, 제3자가 인증을 우회 하거나 인증 방법을 알아내더라도 내부 데이터 접근이 불가능해야한다.

③ 단말기의 분실 및 도난 시 내부규정에 정의된 분실 신고절차에 따라 처리해야하며, 신고의 내용에는 아래의 사항이 반드시 명시되어야 한다.

가. 단말기 정보 (일련번호 등)

나. 단말에 저장되어 있는 주요정보

다. 단말의 보안상태 (장치 기능정지 가능여부 등)

라. 분실자 인적사항 (이름, 연락처, 사번 등)

마. 분실 추정 위치

2. 정보유출 및 위·변조에 대한 대응

① 스마트워크 환경에서 정보의 유출 및 위·변조 사고의 발생 시 아래의 각 사항을 포함한 대응절차를 내부규정에 정의해야 한다.

가. 스마트워크 정보 유출 및 위·변조 사고를 대응하는 담당업무 및 담당자 정의

나. 스마트워크 정보 유출 및 위·변조 신고 절차 및 접수 방법에 대한 정의
다. 스마트워크 정보 유출 및 위·변조로 인한 피해 규모에 대한 대략적 예측 방법에 대한 정의
라. 스마트워크 정보 유출 및 위·변조 사고의 원인분석방법에 대한 정의
마. 스마트워크 정보 유출 및 위·변조 사고의 대응방법에 대한 정의

② 스마트워크환경에서 정보 유출 및 위·변조 사고의 발생 이후 유사한 사고의 재발을 방지하기 위한 사고대응 기록을 면밀히 남기고, 스마트워크 정보보호 관리자는 이를 확인해야 한다.

제4장 스마트워크 이용자 준수사항

제11조(정보자산의 취급 및 관리) 이용자는 정보자산이 적절한 수준의 보호를 받을 수 있도록 하기 위해서는 다음 각 호의 사항에 대해 지속적으로 점검하고 수행하여야 한다.

1. 이용자는 스마트워크용 PC 및 휴대단말기가 보안 위협에 노출되지 않도록 비밀번호를 설정하고 주기적으로 변경해주며, 악성코드의 전파경로로 무선인터넷 인터페이스가 악용될 수 있으므로 블루투스 및 무선랜 기능 등은 사용 시에만 켜놓도록 설정한다.
2. 이용자는 자신이 사용하고 있는 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트하여 사용하고 주기적인 보안점검을 실시해야 한다.
3. 이용자는 정보의 안전한 전송 및 보관을 위해 보안설정 없는 무선랜으로 결재, 기밀자료 열람 등의 민감한 서비스를 이용하지 않도록 한다.

제12조(인식제고) 이용자는 안전한 스마트워크 이용이 이루어질 수 있도록 지속적인 보안 인식제고 활동을 수행해야 한다.

1. 이용자는 단말기 및 관련 설비, 정보 취급방침 등을 숙지할 수 있도록 주기적으로 교육을 받아야 한다.
2. 이용자는 스마트워크 센터 이용, 재택근무, 모바일 오피스 근무 시 정보보호 주의사항 및 침해사고 발생 시 대응방안 등을 반드시 숙지하고 주기적인 교육을 받아야 한다.
3. 이용자는 스마트워크 서비스 제공자가 중요정보의 유출을 방지하기 위해 스마트워크용 PC, 휴대단말기 등에 대한 업무현황 모니터링이 이루어지고 있음을 사전에 인지하고 있어야 한다.

제13조(침해사고 대응) 이용자는 스마트워크 환경에서의 보안 침해사고 발생 시 신속하고 효과적으로 대응해야 한다.

1. 이용자는 단말기를 분실하거나 도난당했을 때 해당기관에 즉시 신고하고, 단말기 내에 저장된 민감한 정보의 외부유출을 방지하기 위한 기술적, 관리적 보호조치를 취해야 한다.
2. 이용자는 스마트워크 센터 및 모바일 오피스 이용, 재택근무 과정에서 발생할 수 있는 정보유출 및 위변조 사고 발생 시 서비스제공자, 관리자 등에게 신속히 연락하여 적절한 기술적, 관리적 보호조치를 취할 수 있도록 한다.

제5장 보 칙

제14조(효력의 개시) 본 권고는 공표한 날부터 시행한다.

제15조(권고의 개정에 관한 사항) 본 권고는 스마트워크 관련 기술의 발전 및 스마트워크 환경에서의 보안 취약성 및 위협 요인, 기타 환경 변화 등에 따라 서비스제공자 및 이용자 등의 의견수렴을 통해 개정할 수 있다.