**사용자보안지침**

소관파트: 정보보안파트

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2017.03.15 제정  2017.11.00 개정 |  |  |  |  |

**제 1 장 총 칙**

**제 1 조 (목적)** 이 지침은 「정보보호규정」에서 위임한 바에 따라 당행의 정보자산을 사용하는 전 임직원 및 제3자(용역, 상주자)에 대하여 보안규정 및 지침을 준수하는데 필요한 최소한의 사항을 정의함으로써 정보자산을 각종 위협으로부터 보호함을 그 목적으로 한다.

**제 2 조 (적용범위**) 이 지침은 당행의 정보자산(단말기, 프린터, E-MAIL 등 유무형 자산)을 사용하는 전 임직원, 외주업체 직원(이하 “사용자”)을 대상으로 한다.

**제 3 조 (용어정의)** 이 지침에서 사용하는 용어 정의는 다음 각 호와 같다.

1. ‘이메일’ : 통신망을 이용하여 컴퓨터에 저장된 정보를 다른 사람에게 전달하거나 받는 시스템을 말한다.

2. ‘악성코드’ : 컴퓨터의 정상적인 동작에 영향을 미치거나 저장된 데이터를 파괴하는 행동을 하는 악성 소프트웨어를 말한다.

3. ‘백신 프로그램’ : 악성코드 프로그램을 탐지 및 제거하고, 손상된 데이터를 치료하는 프로그램을 말한다.

4. ‘정보자산’ : 위협과 취약성으로부터 보호되어야 할 가치가 있는 유무형의 자산을 말한다.

5. ‘단말기’ : 업무용 시스템에 접근하는 PC, 노트북, 가상 PC 및 스마트 기기를 의미하며 서버와 통신망으로 연결되어 데이터를 입력하거나 처리 결과를 출력하는 장치를 포함한다. 또한 단말기는 취급하는 정보와 사용형태 및 통제방법에 따라 다음의 유형으로 분류한다.

가. 중요단말기는 운영 목적의 시스템, DB, 정보보호시스템, 네트워크에 직접 접속 권한이 부여된 ~~금융업무망 시스템에 대한 운영접속 및 개인정보 등의 중요정보를 취급하는~~ 단말기를 말한다.

나. 금융업무망 개발·업무단말기는 코어뱅킹 개발서버 접속, 금융업무망 업무서비스 접속 등 금융업무망 개발·업무 용도로 사용하는 단말기를 말한다.

다. 경영지원망 개발·업무단말기는 채널·인트라넷 개발서버 접속, 경영지원망 업무시스템 접속 등 경영지원망 개발·업무 용도로 사용하는 단말기를 말한다.

라. 경영지원망 운영단말기는 경영지원망 시스템 운영업무 용도로 사용하는 단말기를 말한다.

마. 반출전용 단말기는 장애 대응 등 업무상 불가피한 경우에 외부업무 용도로 사용하는 단말기를 말한다.

6. ‘보조기억매체’ : 단순히 정보를 저장하고 정보의 이동이 가능하도록 지원하는 보조기억매체는 컴퓨터 등 정보통신 시스템에 연결 가능하고 다른 추가 프로세스 없이 해당 매체의 실행만으로 정보를 저장하거나 삭제할 수 있어 누구나 간편하게 사용할 수 있는 저장매체를 말한다.

7. ‘워터마크’ : 무단복사 및 배포 방지를 위해 출력물의 배경에 인쇄되는 그림 또는 글자를 말한다.

**제 2 장 역할 및 책임**

**제 4 조 (정보보안파트)** ① 정보보안파트는 당행의 정보보호 관련 업무를 수행한다.

② 정보보안파트는 사용자 보안 관리에 필요한 보안정책을 수립하고 시행한다.

**제 5 조 (정보보호담당자)** ① 정보보호담당자는 당행의 정보보호 관련 업무에 대한 계획 수립 및 운영, 감독의 실무를 수행한다.

② 정보보호담당자는 각 파트의 사용자보안지침 이행여부를 확인한다.

③ 정보보호담당자는 단말기 보안정책의 수립, 운영 및 모니터링 업무를 수행한다.

**제 6 조 (파트 정보보호관리자)**

① 각 파트장은 해당 파트의 파트 정보보호관리자 업무를 담당한다.

② 파트 정보보호관리자는 소관파트의 사용자보안지침 준수여부 및 단말기 보안정책에 대한 이행여부를 관리하며단말기 보안정책의 예외 사용 요청에 대한 검토 및 승인 업무를 수행한다.

③ 파트 정보보호관리자는 해당 파트의 정보보호 활동을 담당할 파트 정보보호담당자를 지정하여 각 파트의 정보보호 활동 관련 실무 처리를 위임할 수 있다.

**제 7 조 (파트 정보보호담당자)**

① 파트 정보보호당자는 소관파트의 사용자보안지침 이행을 주도한다.

② 파트 정보보호담당자는 보안사고 발생 시 사용자보안지침 및 「보안사고대응지침」에서 정한 바에 따라 대응업무를 수행한다.

③ 파트 정보보호담당자는 소관파트 단말기에 대한 보안정책 이행여부를 점검한다.

**제 8 조 (단말기담당자)** 사내 단말기의 운영 및 관리의 업무를 수행한다.

**제 9 조 (단말기사용자)** ① 단말기보안 유지 및 관리의 책임은 단말기 사용자에 있으며 단말기사용자는 이 지침에서 정한 바에 따라 단말기를 이용하며 관리한다.

② 단말기사용자는 단말기의 도난, 분실, 파손, 정보유출 등에 대한 책임을 진다.

③ 단말기사용자는 당행에서 제공하는 보안프로그램(백신 프로그램 등)을 반드시 설치해야 한다.

**제 3 장 임직원의 임무**

**제 10 조 (임직원 준수사항)** ① 접근이 허가되지 않은 정보 자산에 접근을 시도하거나 정보보호 기능을 우회하려는 시도를 해서는 아니 된다.

② 정보자산을 무단으로 변조하거나 훼손해서는 아니 된다.

③ 정보시스템은 개인 목적이나 이익을 위하여 사용할 수 없으며 업무용으로만 사용하여야 한다.

④ 업무상 취득한 정보를 사전 승인 없이 누설해서는 아니 된다.

⑤ 저작권을 침해할 수 있는 소프트웨어 또는 문서를 소유하거나 이를 통신망을 통하여 무단으로 배포해서는 아니 된다.

⑥ 미 승인 된 정보시스템 기기를 반입해서는 아니 된다.

⑦ 퇴근시나 외근 시와 같이 장시간 자리를 비울 경우 타인에게 노출을 금지하는 정보가 포함된 문서를 개방된 공간에 방치하지 않도록 한다.

⑧ 모든 임직원은 정보시스템의 침해사고 및 보안 사고 등이 발생하였거나 발생징후를 감지하였을 경우 이를 지체 없이 정보보호담당자 또는 정보보안파트에 신고하여야 한다.

⑨ 임직원은 이 지침을 포함하여 자신의 직무와 관련된 각종 정보보호 관련 규정을 준수하여야 하며, 이를 위반할 경우 「인적보안지침」에 근거하여 징계 처분을 받을 수 있다.

⑩ 임직원 및 외주인력은 퇴사시(외주인력의 경우 외부업무 종료 시) 「인적보안지침」 및 「외부주문보안지침」에서 정한 바에 따라 사용하던 정보시스템의 계정 및 접근권한, 물리적 접근권한, 장비 등을 반납하여야 한다.

**제 4 장 인터넷 관리**

**제 11 조 (인터넷 보안)** ① 망분리 환경에서 인터넷 사용은 다음 각 호의 통제사항을 준수한다.

1. 금융업무망 개발·업무단말기의 인터넷 사용 차단

2. 중요단말기의 인터넷 사용 차단

3. 경영지원망 개발·업무단말기의 인터넷 사용 허용, 글쓰기 용량제한 및 파일 첨부 불가

4. 경영지원망 운영단말기의 인터넷 사용 차단

② 근무 시간 중 업무와 관련이 없는 인터넷 사용을 해서는 아니 된다.

③ 인터넷에서 파일을 다운로드 한 경우 이를 실행하기 전에 반드시 바이러스의 감염 여부를 확인하여야 한다.

④ 임의로 외부 네트워크(T-login, Wibro, 테더링, AD-hoc 등)를 사용하기 위한 장치를 설치하여서는 아니 된다.

⑤ 당행은 중요정보 유출 및 법규 위반 등을 방지하기 위해 인터넷 사용 기록은 저장 및 열람할 수 있다.

**제 12 조 (이메일·메신저 사용 원칙)** ① 이메일·메신저를 불법적인 용도, 불순한 목적, 또는 개인적인 용도로 사용해서는 아니 된다.

② 당행 및 제3자의 지적재산권, 저작권을 침해하는 내용, 명예 훼손, 사기, 바이러스 유포 등의 불법적인 행위와 관련해서 이메일을 사용해서는 아니 된다.

③ 타인의 이메일 계정을 사용하여서는 아니 된다.

④ 발신인이 확실하지 않거나 바이러스를 포함한 것으로 의심되는 메일은 읽어서는 아니되며, 파트 정보보호담당자에게 즉시 통보한다.

⑤ 허가된 메신저나 이메일 외 사용을 원칙적으로 금지한다.

⑥ 당행은 중요정보 유출 및 법규 위반 등을 방지하기 위해 사용자의 업무용 이메일·메신저의 송·수신 정보 등의 로그기록은 저장 및 열람할 수 있다.

**제 5 장 단말기 보안**

**제 13 조 (단말기 관리)** ① 단말기는 사용자별로 사용함을 원칙으로 한다.

② 단말기에 이용자 정보 등 주요정보를 보관하지 아니한다. 다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유 및 보관기간을 정하여 ~~책임자~~소속 파트장의 승인을 받아야 한다.

③ 단말기 및 단말기 내의 정보는 인가된 업무상의 목적을 위해서만 사용하여야 한다. 다만, 업무상 불가피하게 공용 단말기의 사용이 필요한 경우, 공용 단말기는 관리자와 사용자를 지정해야 하며, ~~정보보안~~ 소속 파트장과 정보보안파트 파트장의 승인 후 사용 가능하다.

④ ~~공용~~ 단말기 관리자는 공용 단말기 사용자를 식별, 관리하여야 하며 공용 단말기에는 원칙적으로 당행의 내부정보를 저장하지 않아야 한다.

⑤ 당행 업무 종료 후 퇴근시 단말기 전원을 꺼야 한다. 다만, 업무상 필요한 경우는 그렇지 않을 수 있다.

⑥ 단말기보안 예외적용은 「사용자단말기보안~~가이드~~업무매뉴얼」에 따라 정보보안 파트의 예외 승인을 득한 후 적용할 수 있다.

⑦ 업무용 단말기 중 중요단말기는 다음 각 호와 같다.

1. 운영 목적의 시스템, DB, 정보보호시스템, 네트워크에 직접 접속 가능한 단말기

2. 고객정보 등에 접근 및 저장이 가능하여 파트장이 별도로 지정한 단말기

3. CISO가 필요하다 인정하여 별도로 지정한 단말기

⑧ 중요단말기는 ~~가상단말기로 금융업무망~~ 유선 네트워크 접속을 통해 사용하며 보안통제 방안은 다음 각 호와 같다.

1. 인터넷 사용불가

2. 화면보호기 적용

3. 보조기억매체 통제

~~4. 메신저 사용불가~~

4. 외부반출불가

5. 중요정보 보관은 최소화, 불가피하게 보관 시 암호화 저장

6. 당행 보안 프로그램 임의해제 및 삭제 불가

7. 그룹웨어 접속금지

단, 정보접근이 차단되거나 보호조치가 적절하다고 인정한 경우는 예외로 함

~~⑨ 중요단말기는 반출이 불가하다.~~

**제 14 조 (망분리 운영관리)** ① 당행은 금융업무망과 경영지원망이 물리적으로 분리되어 있으며, ~~중요단말기~~금융업무망 가상단말기, 금융업무망 개발**·**업무단말기, 경영지원망 개발**·**업무단말기, 경영지원망 운영단말기로 구분한다.

② 단말기 유형 별 주요 통제사항은 다음 각호와 같다.

1. ~~중요단말기는~~금융업무망 가상단말기는 망분리 대상으로서 인터넷 접속이 금지되며, 금융업무망 단말기에서 유선 네트워크로만 VDI전환이 가능, 가상 OS 주기적 초기화, 메일 송수신금지, 그룹웨어 접속금지 등의 통제가 적용된다.

2. 금융업무망 단말기는 망분리 대상으로서 인터넷 접속이 금지되며, 운영서버 직접접속 금지, 개인정보 취급 금지 등의 통제가 적용된다.

3. 경영지원망 개발·업무 단말기는 망분리 비 대상으로 인터넷 접속이 가능하나, 인터넷을 통한 글쓰기나 파일첨부 등은 통제된다.

4. 경영지원망 운영단말기는 경영지원망 시스템 운영업무 용도로 사용하며, 인터넷 접속금지 등의 통제가 적용된다.

③ 망간자료전송시스템을 통해 망간 파일~~자료~~전송(FTC)이 가능하다.~~하며, 스트림 전송과 파일전송(FTC)로 구분된다.~~

④ 망간 자료전송 방법은 업무목적에 따라 적용 및 운영되며, 망간 자료전송은 「사용자단말기보안~~가이드~~업무매뉴얼」에서 정한 바에 따라 소속~~관~~ 파트장의 승인을 득하여야 한다.

**제 15 조 (소프트웨어 설치 및 관리)** ① 단말기에는 당행의 보안 소프트웨어를 반드시 설치하여야 하고, 임의로 삭제하거나 변경해서는 아니 된다.

② 소프트웨어 설치 시 다음 각 호의 사항을 따른다.

1. 단말기는 지적재산권을 준수하여 정품 소프트웨어만을 설치하여야 한다.

2. 정보시스템을 침해하거나 우회할 수 있는 프로그램을 임의로 설치해서는 아니된다.

3. 원격접속 소프트웨어의 설치 및 사용은 제한한다. 다만, 업무상 부득이한 경우 ~~파트 정보보호관리자정보보호최고책임자~~ 소속 파트장과 정보보안파트 파트장의 승인을 득한 후 인가된 원격접속 소프트웨어에 한하여 설치 및 사용이 가능하다.

**제 16 조 (단말기 보안패치 관리)** ① 단말기 보안패치는 패치관리시스템을 통하여 처리하여야 하며 인터넷을 통한 임의의 패치는 원칙적으로 금지한다.

② 패치관리시스템을 통해 제공된 단말기 보안패치는 즉각 수행한다.

**제 17 조 (단말기 하드웨어 설치 및 관리)** ① 허가되지 않은 단말기의 임의 설치를 금지하며 단말기관리자는 허가된 단말기를 기록 관리한다.

② 단말기에는 정보시스템을 침해하거나 우회할 수 있는 하드웨어를 임의로 설치해서는 아니 된다.

**제 18 조 (접근통제)** ① 임직원은 단말기의 계정과 비밀번호가 타인에게 노출되지 않도록 다음 각 호와 같은 사항을 준수해야 한다.

1. 비밀번호를 타인과 공유하거나 알려서는 안 되며, 유출∙분실∙도난 등으로부터 안전하게 관리할 책임이 있다.

2. 비밀번호는 영문 대문자, 영문 소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 설정한다

3. 연속적인 숫자 또는 문자나 생년월일, 주민등록번호, 전화번호 등 추측하기 쉬운 개인정보 및 계정명과 같은 비밀번호는 사용할 수 없다.

4. 비밀번호는 분기 1회 이상 변경하여야 한다.

5. 최초 로그인 시 임의로 부여된 비밀번호는 반드시 변경하여야 한다.

6. 비밀번호가 노출된 것으로 의심될 경우 즉시 비밀번호를 변경해야 한다. 또한 이로 인하여 해킹 피해가 발생한 것으로 의심되는 경우 이를 정보보안 파트에 신고하여야 한다.

② 10분 이상 단말기 미 사용 시 화면보호기가 작동되고 재시작 시 비밀번호를 입력하는 잠금 장치를 설정해야 한다.

③ 단말기의 회사 네트워크 사용은 반드시 네트워크접속통제시스템을 통해 인증을 받은 후 사용할 수 있도록 하며, 인증 받지 않거나 보안 무결성에 위배된 단말기는 네트워크 접속이 차단 되어야 한다.

④ 임직원은 업무상 필요한 경우를 제외하고는 데이터 공유를 하지 않는다. 단, 업무수행 상 부득이한 경우에는 ~~소관 파트장의 승인과 정보보호담당자의 합의를~~ 소속 파트장과 정보보안파트 파트장의 승인을 득한 후 공유 폴더 접근허용 패스워드 및 사용권한을 설정하여 사용하여야 한다.

**제 19 조 (악성코드 감염 방지 및 감염 시 조치 사항)** ① 주기적인 악성코드 검색을 위해 당행에서 제공한 백신 프로그램을 모든 단말기에 설치하여야 하며, 임의로 삭제하거나 기능을 정지하여서는 아니 된다.

② 중요단말기를 포함, 모든 단말기는 악성코드 감염여부를 주기적(일 1회)으로 점검한다.

③ 백신프로그램은 항상 최신의 정보를 포함하도록 업데이트해야 한다.

④ 이메일, 전자게시판 등에서 받은 응용 프로그램이나 새로운 응용 프로그램 사용 시 백신프로그램으로 진단 및 치료 후 사용한다.

⑤ 업무 목적으로 승인된 보조기억매체 사용 시 백신프로그램으로 진단 및 치료 후 사용한다.

⑥ 단말기의 오동작 등 자신이 관리하고 있는 단말기의 악성코드 감염이 의심되는 경우, 단말기의 네트워크 접속을 차단, 분리하고 정보보호담당자에게 즉시 통보한다.

**제 20 조 (부정 사용 금지)** ① 당행의 허가없이 내부통신망과 연결된 단말기를 외부통신망에 우회하여 무단 접속하는 것을 금지한다.

② 전자적 침해행위를 하여서는 안되며, 전자적 침해행위로 인하여 전자금융기반 시설이 교란ㆍ마비되는 등의 사고가 발생한 때에는 「보안사고대응지침」에서 정한 바에 따라 파트 정보보호담당자 또는 정보보호담당자에게 즉시 전달한다.

**제 21 조 (정보보호 침해사고 통보 및 대응)** ① 단말기 관련 정보보호 침해사고 발생 시 「보안사고대응지침」에서 정한 바에 따라 대응해야 한다.

② 단말기 내 소프트웨어 오동작 및 손상 등으로 인해 정보보호 사고가 의심될 경우, 파트 정보보호담당자에게 즉시 통보한다.

③ 단말기에 접근하기 위해 사용되는 비밀번호가 노출되었거나 노출이 의심되는 경우, 비밀번호를 즉시 변경한다.

**제 22조 (보조기억매체 사용 통제)** ① 단말기에서의 보조기억매체 사용은 원칙적으로 금지한다. 다만, 업무목적에 따른 보조기억매체 사용은 「사용자단말기보안~~가이드~~업무매뉴얼」에서 정한 바에 따라 ~~소관 파트장의 승인과 정보보호담당자의 합의를~~ 소속 파트장과 정보보안파트 파트장의 승인을 득한 후 사용할 수 있다.

② 정보보호담당자는 정기적으로 보조기억매체의 보유현황 및 관리실태를 점검한다.

**제 23조 (단말기 반·출입 금지)** ① 단말기의 임의 반·출입은 금지한다. 단 업무목적상 반·출입이 필요한 경우, 「물리적보안지침」에서 정한 바에 따른다.

**②** 반출전용 단말기의 경우, 장애 대응 등 상시 반출이 요하는 경우에 한하여 사전 승인을 거쳐 외부 반출이 가능하다.

**제 24조 (단말기 교체 및 반납)** ① 단말기 교체 시, 기존 저장된 데이터는 복구가 불가능한 방법을 사용하여 삭제한 후 교체하여야 한다.

② 인사발령이나 퇴사 등의 이유로 단말기 반납 시, 기존 저장된 데이터는 복구가 불가능한 방법을 사용하여 삭제한 후 단말을 반납하여야 한다.

**제 25조 (단말기 유지보수 및 폐기)** ① 하드웨어의 폐기를 위한 단말기의 외부 반출 시, 기존 저장된 데이터는 복구가 불가능한 방법을 사용하여 삭제한 후 반출하여야 하며, 단말기담당자는 그 현황을 기록ㆍ관리하여야 한다.

② 하드웨어의 유지보수를 외부업체에 의뢰 하여 수행할 경우 인사/경영지원파트는 계약 시 비밀유지서약 등의 보호 대책을 적용한다.

③ 외부업체에 의뢰 하여 하드웨어 폐기 시, 천공 폐기 등의 데이터 복구가 불가능한 방법을 사용하여야 한다. 또한 단말기담당자는 폐기 시 반드시 입회하여 폐기된 하드웨어의 증적 사진 등의 기록을 남겨야 한다.

**제 6 장 사무실 보안**

**제 26조 (출력물 보안)** ① 출력물은 보안을 위하여 워터마크를 적용한다.

② 프린터 팩시밀리, 복사기 등 사무자동화기기에 출력된 문서는 즉시 회수하여 방치되지 않도록 하여야 하며, 사무자동화기기의 출력물에 대한 관리 책임은 출력자에게 있다.

③ 중요 정보가 인쇄된 인쇄물은 이면지로 사용하여서는 아니되며 용도 폐기 시 파쇄기를 이용하여 해당 인쇄물을 파쇄 하도록 한다.

④ 계정 비밀번호 등 타인에게 노출을 금지하는 정보가 포함된 문서를 책상에 방치하지 않도록 한다.

⑤ 당행은 중요정보 유출 및 법규 위반, 전산기기의 오·남용 등을 방지하기 위해 출력물에 대한 내역을 저장 및 열람할 수 있다.

**부칙 (2017. 03. 15)**

**제 1 조 (시행일)** 이 지침은 2017.03.15 부터 시행한다. 단, 은행업 인가를 전제로 한 사항은 당행이 은행업 본인가를 받은 날로부터 적용한다.

**부칙 (2017. 06. 00)**

**제 1 조 (시행일)** 이 지침은 2017.06.00 부터 시행한다.