유형	AS-IS	TO-BE
변경	보안 조치 서비스 은행 보안 조치 4. 6개월간 HSBCnet에 로그인하지 않은 지정 이용자는 서비스 이용자의 보안 조치의 일환으로 자동으로 사용이 정지된다.	보안 조치 서비스 은행 보안 조치 3. 서비스 은행 보안 조치의 일부로 서비스 이용자가 권한을 준 이용자(이하 "지정 이용자")가 6 개월 간 HSBCnet 에 로그인하지 않은 경우 자동으로 사용이 일시 정지될 수 있다. 서비스 이용자의 어떠한 지정이용자도 18 개월 간 HSBCnet 에 로그온하지 않는 경우 HSBCnet 프로파일 역시 일시 정지될 수 있다. 4. 생체정보를 활용한 인증 방법(예: 지문 스캔 또는 얼굴 인식)으로 모바일 장치에서 E-Channel에 접근하는 경우, 해당 모바일 장치에 어플리케이션을 제공하는 서비스 은행 및 관련 HSBC 계열사는 장치의 보안과 관련된 우려 사항이 있는 경우, 필요에 따라, 통지 없이 언제든지 생체정보를 활용한 인증 기능을 삭제할 수 있는 권한을 가진다. 일반적인 경우, 기존의 다른 방법을 사용한 모바일 장치에서의 인증이 가능하다.
변경	서비스 이용자 보안 조치 **6. 서비스 이용자는 다음을 이행해야 한다.** (a) 만일 지정 이용자의 인증 정보 전체 또는 일부가 보안 위험에 처했다고 판단되는 경우, 즉시 적절한 보호 조치를 취한다. (b) 만일 지정 이용자의 인증 정보가 보안 위험에 처했다고 판단되는 경우 해당 계좌와 지정 이용자의 최근 활동을 검토하여 신속히 서비스 은행에 문제점을 통지한다. 그리고, (c) 서비스 이용자의 계좌 그리고 지정 이용자의 활동을 정기적으로 검토하여, 문제가 없는지 확인하고 문제가 있는 경우 이를 서비스 은행에 즉시 보고한다.	서비스 이용자 보안 조치 **5. 서비스 이용자는 다음을 이행해야 한다.** (a) 만일 지정 이용자의 인증 정보 전체 또는 일부가 보안 위험에 처했다고 판단되는 경우, 즉시 적절한 보호 조치를 취한다. (b) 만일 지정 이용자의 인증 정보가 보안 위험에 처했다고 판단되는 경우 해당 계좌와 지정 이용자의 최근 활동을 검토하여 신속히 서비스 은행에 문제점을 통지한다. (c) 서비스 이용자의 계좌와 지정 이용자의 활동 및 권한을 정기적으로 검토하여, 문제가 없는지 확인하고, 문제가 있는 경우 이를 서비스 은행에 즉시 보고한다.
변경	7. 서비스 이용자는, 지정 이용자가 퇴사하는 경우 또는 지정 이용자 및 그들의 권한에 대한 우려 사항이 있는 경우 해당 지정 이용자의 E-Channels 사용을 즉시 중단 시킬 수 있다. 서비스 이용자는 지정 이용자가 휴가 중이거나 퇴사하는 경우에도, 해당 지정 이용자의 보안 인증 정보 또는 장치(해당 지정 이용자에게 발급된)가 다른 지정 사용자에게 이전 또는 공유되지 않도록 한다.	6. 서비스 이용자는 지정 이용자가 퇴사하는 경우 해당 지정 이용자를 E-Channel 프로파일에서 즉시 삭제해야 한다. 또한 서비스 이용자는 지정 이용자 및 그들의 권한에 대한 우려 사항이 있는 경우 해당 지정 이용자의 E-Channels 사용을 즉시 중단시켜야 한다. 서비스 이용자는 보안 인증 정보 또는 장치가 이를 배정 받은 해당 지정 이용자에 의해서만(서비스 이용자가 권한을 준 제3의 서비스 제공자를 제외) 사용 될 수 있도록 해야 한다.
변경	8. 서비스 이용자는 개인이 하나 이상의 사용자 이름 또는 보안 인증정보를 보유하지 않도록 한다.	7. 서비스 이용자는 HSBC 그룹이 요청하는 경우에 지정 이용자가 정확하고 완전하며 축약되지 않은 세부 정보를 제공하도록 해야 한다. 또한 서비스 이용자는 지정 이용자가

		이러한 정보를 정기적으로 검토하고 변경이 있을 때마다 업데이트하며, 이용자 이름이나 보안 자격 증명을 복수로 유지하지 않도록 해야 한다.
변경	11. 서비스 이용자는, 보호 수준을 최신으로 유지하고 감독기관 및 업계의 모범 관행 수준에 맞는 보호 조치를 유지하기 위해 내부 보안 조치를 정기적으로 검토한다. 이러한 검토 활동에는 악성코드로부터의 보호, 네트워크 제한, 물리적 접근 제한, 원거리 접근 제한, 컴퓨터 보안 세팅, 부적절한 사용 모니터링 등이 포함된다. 12. 서비스 이용자는 수락 가능한 웹 브라우저와 멀웨어(Malware) 수집을 피하는 방법을 포함하는 이메일 사용에 대한 지침을 포함하는 내부 절차를 수립 및 운영해야한다	10. 서비스 이용자는 내부 보안 조치를 채택하고 정기적으로 이를 검토하여 감독 규정 및 업계 모범 관행에 따라 최신 상태의 보안이 이루어질 수 있도록 해야 한다. 이는 멀웨어 보호, 네트워크 제한, 물리적 액세스 제한, 원격 액세스 제한, 컴퓨터 보안 설정, 부적절한 사용에 대한 모니터링, 허용되는 웹 브라우저 및 멀웨어 방지 방법을 포함한 이메일 사용에 대한 지침 등을 포함한다.
변경	14. 만일 지정 사용자가 모바일 기기를 통해 E-Channel에 접근하는 경우, 서비스 이용자는 해당 지정 이용자에게 다음을 요청해야 한다. (a) E-Channels에 로그온한 이후 해당 이동전화기를 방치해 두어서는 안됨. (b) 지정 이용자가 E-Channels 접속을 종료하는 경우 '로그아웃' 버튼을 클릭하여야 함. 그리고, (c) 해당 모바일 기기의 자동 비밀번호 잠금 기능을 활성화 하여야 함.	12. 만일 지정 사용자가 모바일 기기를 통해 E-Channel에 접근하는 경우, 서비스 이용자는 해당 지정 이용자에게 다음을 요청해야 한다. (a) E-Channels에 로그온한 이후 해당 모바일 기기를 방치해 두어서는 안됨. (b) 지정 이용자가 E-Channels 접속을 종료하는 경우 '로그아웃' 버튼을 클릭하여야 함. (c) 해당 모바일 기기의 자동 비밀번호 잠금 기능을 활성화하여야 함. (d) E-Channel 접근에 사용되는 모바일 기기를 타인과 공유하지 말아야 함. (e) 해당 기기에서의 바이오 인증(예. 얼굴, 지문, 음성, 망막)은 본인만 등록되어 있어야 함. (f) 15조에 명시된 인증 방법으로 사용되어서는 안되는 기기에 대한 등록 해제 조치를 취하여야 함. (g) IOS 탈옥(jailbroken), 안드로이드 루팅(rooted) 등 보안 해제된 모바일 기기를 통해 E-Channel에 접근하지 않아야 함.
변경	**16.** 서비스 이용자는 지정 이용자가 모바일 기기에서 제공되는 바이오 인증(예. 지문 스캔, 얼굴 인식)을 통해 E-Channel에 접근할 수 있으며, 이러한 접근 방식에는 노출 및 무단 접근 가능성(예. 가까운 가족 구성원을 통한 무단 접근) 등의 리스크가 있음을 인식하여야 한다. 또한 서비스 이용자는 지정 이용자가 바이오 인증을 위해 모바일 기기에 정보를 등록 할 때 반드시 본인의 바이오 정보를 등록 하도록 해야 한다.	14. 서비스 이용자는 모바일 기기를 통해 E-Channel에 접근하는 지정 이용자가 해당 기기를 사용하여 다양한 활동을 수행할 수 있음을 인식하여야 한다. 이러한 활동에는 데스크 탑 컴퓨터를 이용한 별도의 E-Channel 세션에서 이루어지는 활동을 인증하기 위해 (보안 장치 대신) 모바일 기기를 사용하는 것을 포함한다. 15. 지정 이용자가 모바일 기기에서 사용 가능한 바이오 인증(예. 지문 스캔, 얼굴 인식)을 통해 E-Channel에 접근하는 경우, 서비스 이용자는 이러한 인증 방식에는 노출 및 무단 접근 가능성(예. 가까운 가족 구성원을 통한 무단 접근) 등의 리스크가 있음을 인식하여야 한다.