IBM Security
리더십 사고의 백서

BYOD（회사 업무에 직원 개인의 통신기기를 사용할 수 있게 하는 방침）10대 규칙

사용자가 업무를 위해 개인 장치를 사용할 때 기업 데이터 보호 방법 알아보기

IBM

BYOD를 허용해야 합니까?

작업장에 들고가는 모바일 장치가 급속히 증가하는 것은 수많은 IT 리더에게 신의 중재와 같은 일입니다. 모바일 장치와 앱을 통해 살고 있는 방식, 즉, 의사소통, 여행, 쇼핑, 업무 등의 방법이 변화했습니다. 이러한 이동성 전환은 매우 급진적이고 혁명적이며, 이러한 장치 없이 사는 삶은 상상하기 힘듭니다. BYOD（회사 업무에 직원 개인의 통신기기를 사용할 수 있게 하는 방침）가 탄생했고 직원들은 열병에 걸린 듯 따르고 있습니다.

이런 일이 없었던 척하거나 "직원들이 이런 짓을 못하게 막고 있어요"라고 말하는 것은 어불성설입니다. 사실, 이미 사용 중이고 승인 여부에 관계없이 비준수 장치를 몰래 네트워크로 계속 가져오고 있을 가능성이 큽니다. 2016년까지 대다수의 기업 직원들이 업무를 위해 자신들의 스마트폰과 태블릿을 사용하도록 승인을 받게 될 것입니다.

이런 의문이 들 수도 있습니다. 개인 앱과 장치를 사용하길 원하는 직원들을 지원하는 동시에 기업 데이터를 보호하는 안전한 환경에서 생산성을 유지하게 할 것입니까? *BYOD（회사 업무에 직원 개인의 통신기기를 사용할 수 있게 하는 방침）10대 규칙*은 평화롭고, 보호받으며, 생산적인 모바일 환경을 만드는 방법이 무엇인지 보여줍니다.

BYOD（회사 업무에 직원 개인의 통신기기를 사용할 수 있게 하는 방침）10대 규칙

1. 기술 조달 전 정책 생성
2. 기업 자원에 액세스하는 장치 발견
3. 간편한 등록
4. 무선으로（Over-the-Air）장치 구성
5. 사용자가 스스로 문제를 처리하도록 지원
6. 개인 정보 비공개 유지
7. 개인 정보와 기업 데이터 분리 유지
8. 데이터 사용량 관리
9. 장치의 비준수 사항을 지속적으로 모니터링
10. BYOD로 인한 투자수익률（ROI）확보

1. 기술 조달 전 정책 생성

다른 IT 프로젝트처럼, 정책은 기술보다 선행되어야 합니다. 클라우드에서도 말이죠. 효과적으로 직원 소유 장치에 대한 모바일 장치 관리（MDM）기술을 사용하려면 정책에 의존해서 결정해야 합니다. 이러한 정책은 IT에만 영향을 미치지 않습니다. 인사부, 법무부, 보안 부서 등 생산성의 이름으로 모바일 장치를 사용하는 비즈니스 부서라면 중요한 의미를 가지고 있습니다.

모든 비즈니스 라인들이 BYOD 정책의 영향을 받았기 때문에 IT 진공 상태에서 생성될 수 없습니다. 사용자의 다양한 요구사항과 함께, IT는 모든 정책 생성 부분을 보장해야 합니다.

올바른 BYOD 정책은 없지만, 몇 가지 고려해야 할 질문사항이 있습니다.

- **장치:** 어떤 모바일 장치를 지원합니까? 특정 장치만 지원합니까? 아니면 직원이 원하는 장치라면 지원됩니까?
- **데이터 계획:** 조직이 데이터 계획에 전적으로 자금을 지불합니까? 연금을 발행합니까? 아니면 직원이 지출 보고서를 제출합니까?
- **규정 준수:** 여러분의 조직이 보호해야 하기 위해 어떤 규정으로 데이터를 관리합니까? 예를 들어, HIPAA（Health Insurance Portability and Accountability Act）는 실행하는 데이터 주체를 보유한 장치 상의 기본 / 암호화를 요구합니다.
- **보안:** 어떤 보안 조치가 필요합니까（암호 보호, 탈옥/루팅된 장치, 악성 프로그램 방지 앱, 암호화, 장치 제한, iCloud 백업）?
- **애플리케이션:** 어떤 앱이 금지되었습니까? IP 스캔, 데이터 공유, Dropbox?
- **합의서:** 기업 데이터가 있는 직원 장치를 위한 AUA（Acceptable Usage Agreement, 허용 가능 사용량 합의）가 있습니까?
- **서비스:** 어떤 종류의 자원으로 직원이 이메일에 액세스할 수 있습니까? 특정 무선 네트워크 또는 VPN입니까? CRM입니까?
- **개인 정보 보호 정책:** 직원 장치에서 어떤 데이터를 수집합니까? 수집하면 안 되는 개인 정보는 어떤 것입니까?

BYOD의 한계에 대해서는 의문을 가질 게 없습니다. 장치를 어떻게 사용하고 IT가 어떻게 실질적으로 이러한 요구사항을 충족할 수 있는지에 대한 솔직하고 정직한 대화 방법이 있어야 합니다.

2. 기업 자원에 액세스하는 장치 발견

이런 상황을 상상해 봅시다. 회사가 100개 이상의 장치를 지원한다는 가정하에 MDM 솔루션을 사용하기 시작했습니다. 장치 유형 및 사용자의 정교한 스프레드시트를 유지했지만 이는 놀라울 일도 아닙니다. 그러나, 보고서를 보기 위해 이동할 경우 200개 이상의 장치가 나타납니다. 사실 이 시나리오는 허구가 아니라 실제 사례입니다. 이런 시나리오는 여러분이 상상하는 것보다 훨씬 많이 발생합니다.

부정하지 마십시오. 모르면 화를 자초할 수 있습니다. 전략을 결정하기 전 모바일 장치 사용자 수라는 현재 환경을 이해하셔야 합니다. 이를 위해 지속적으로 이메일 환경과 의사소통할 수 있는 도구가 필요하며, 기업 네트워크에 연결된 모든 장치를 감지해야 합니다. ActiveSync가 메일함을 위해 켜지면 보통 IT 지식 없이 여러 장치를 동기화하는 장벽은 일반적으로 없다는 사실을 잊지 마십시오.

모든 모바일 장치를 모바일 이니셔티브에 통합해야 하며, 소유자는 새로운 보안 정책이 실시된다는 점을 알아야 합니다.

3. 간편한 등록

복잡하면 준수하지 않게 됩니다. 등록하기 위해 장치를 식별할 경우, 귀하의 BYOD 프로그램은 사용자가 등록하기 간편하고 수고스럽지 않은 기술을 사용해야 합니다. 이러한 프로세스는 간편하고 보호되어야 하며, 동시에 장치를 구성해야 합니다.

완벽한 시나리오는 사용자가 매우 중요한 AUA 수락 등 장치에서 생성되는 MDM 프로필로 이어지는 이메일 링크 또는 텍스트를 따르는 것입니다.

화합을 지원하는 혼전 약속으로서 BYOD와 AUA의 결혼으로 여기십시오.

지침은 기존 사용자가 BYOD 프로그램에 등록하도록 도움을 주어야 합니다. 기존 사용자가 ActiveSync 계정을 지워 장치상의 기업 데이터를 분리하고 관리할 수 있도록 하는 것이 좋습니다. 새 장치는 새로운 프로필로 시작해야 합니다.

IT의 관점에서 보면 여러분은 기존 장치를 대량 등록하거나 사용자가 스스로 장치를 등록할 수 있게 하는 능력이 필요합니다. 또한 일회용 암호 등의 기본 인증 프로세스로 직원을 인증하거나 Active Directory/LDAP 등 기존 기업 디렉토리를 사용해야 합니다. 기업 자원에 액세스하려는 새 장치는 격리되어야 하고 IT에서는 이에 대해 알아야 합니다. 이는 IT에 승인될 경우 적절한 등록 워크플로우를 차단하거나 실시하는 유연성을 제공하며, 기업 정책을 준수하도록 도움을 줍니다.

4. 무선으로 (Over-the-Air) 장치 구성

BYOD 정책 및 MDM 솔루션에서 하지 말아야 할 것이 한 가지라도 있다면, 더 많은 사용자가 헬프데스크를 찾게 됩니다. 귀하의 장치를 무선으로 (Over-the-Air) 구성해 IT 및 비즈니스 사용자를 위한 효율성을 최적화해야 합니다.

사용자가 AUA를 수락한다면, 여러분의 플랫폼은 프로필, 인증서, 직원이 다음 사항에 액세스해야 하는 설정을 제공해야 합니다.

- 이메일, 연락처 및 캘린더
- VPN 및 Wi-Fi
- 기업 문서 및 컨텐츠
- 내부 및 공용 앱

이 시점에서, 사용자는 또한 특정 애플리케이션에 대한 액세스를 제한하고 데이터 사용량이나 월별 한도를 초과할 경우 경고를 발생시키는 정책을 생성하게 됩니다.

5. 사용자가 스스로 문제를 처리하도록 지원

그리고 여러분은 스스로 한 일에 안도할 것입니다. 사용자는 작동하는 장치를 원하며, 여러분은 헬프데스크에서 보내는 시간을 최대한 줄이고 싶을 것입니다. 견고한 셀프 서비스 플랫폼은 사용자가 다음 사항을 수행하도록 합니다.

- PIN 및 암호는 직원이 현재 사항을 잊었을 경우 재설정됩니다
- 웹 포털에서 손실된 장치를 맵핑 통합을 사용해 위치 검색
- 장치를 원격으로 지우고 민감한 기업 데이터 삭제

보안, 기업 데이터 보호 및 준수는 모두가 감당해야 할 일입니다. 이는 직원에게 삼키기 어려운 알약과도 같겠지만, 협력 없이는 위험을 완화할 기회 조차 없습니다. 셀프 서비스 포털은 직원이 왜 준수하지 못할 수 있는지 이해하도록 도움을 줄 수 있습니다.

6. 개인 정보 비공개 유지

물론, BYOD 정책은 단지 기업 데이터 보호에 관한 것이 아닙니다. 잘 만들어진 BYOD 프로그램은 개인 직원 데이터를 IT 등 다른 요소로부터 보호합니다. 개인 식별 정보 (PII) 는 사람의 식별, 연락 또는 위치 확인에 사용할 수 있습니다. 일부 개인정보 보호 법률은 이러한 데이터를 기업에서 열람하지 못하도록 방지합니다. 개인정책 보호 정책에 대해 직원과 의사소통하고 어떤 데이터를 모바일 장치에서 수집할 수 없는지 확실히 매듭 지으십시오. 예를 들어, MDM 솔루션은 다음 사항 등 어떤 정보에 액세스가 가능한지 분석할 수 있어야 합니다.

- 개인 이메일, 연락처 및 캘린더
- 애플리케이션 데이터 및 텍스트 메시지
- 통화 기록 및 음성메일

반대로, 사용자가 여러분이 무엇을 수집하고, 어떻게 사용할 것이며, 왜 이익이 되는지 알려 주십시오.

고급 MDM 솔루션은 개인정보 보호 정책을 개인정보 보호 설정으로 전환해 장치 상의 위치 및 소프트웨어 정보를 숨길 수 있습니다. 이는 기업에서 스마트폰 및 태블릿에 있는 개인 정보를 열람하지 못하게 방지함으로써 PII 규정을 충족하게 하고 직원에게 추가로 편의를 제공합니다. 예를 들면 다음과 같습니다.

- 관리자가 개인 애플리케이션을 열람하지 못하게 제한하도록 보하는 앱 인벤토리 비활성화.
- 위치 서비스를 비활성화해 물리적 주소, 위치 좌표, IP 주소 및 Wi-Fi SSID 등의 위치 지표로 액세스 방지.
- 투명성과 명확성은 중요한 표어입니다. 각 개인이 규칙에 대해 알 때 BYOD 정책에 대한 반감이 적습니다.

7. 개인 정보와 기업 데이터 분리 유지

IT 및 사용자가 BYOD를 수용하는 합의 사항으로 정한 경우, 생일파티 사진이나 위대한 미국 소설과 같은 개인 정보는 생산성 앱과 분리되어야 합니다.

직원이 조직을 그만두기로 한 경우, 간단하게 명시된 기업 앱, 문서 및 기타 자료는 IT가 보호해야 하며, 개인 이메일, 앱 및 사진은 기업 IT가 손을 대지 말아야 합니다.

이렇게 자유로운 접근법에 감사함을 느끼는 것은 사용자뿐 아니라 IT도 마찬가지입니다. 결과적으로 삶이 대단히 쉬워질 가능성이 있습니다. 이러한 접근법을 활용해 IT는 직원이 회사를 그만둘 시 선택적으로 기업 데이터를 지울 수 있습니다. 상황에 따라, 직원이 장치를 분실하면, 전체 장치가 지워질 수 있습니다. 진정한 MDM 솔루션으로 여러분에게 선택의 기회를 제공합니다.

일부 86%의 장치 삭제만 선택할 수 있으며, 기업 데이터만 삭제됩니다.

8. 데이터 사용량 관리

일반적으로 BYOD 정책은 통신 회사의 IT에서 발생하는데 수많은 회사에서는 과도한 요금 발생을 방지하기 위해 아직도 직원이 데이터 사용을 관리하는 방법으로 운영하고 있습니다.

데이터 계획 비용을 지불할 경우 이러한 데이터를 추적하고 싶을 수 있습니다. 비용을 지불하지 않는다면 사용자가 현재 데이터 사용량을 추적하도록 도움을 주고 싶을 수도 있습니다. 장치 상에서 네트워크 내 그리고 로밍 데이터 사용량을 추적하고 사용자가 데이터 사용량의 임계값을 넘을 경우 알림을 생성할 수 있어야 합니다.

로밍 및 네트워크 내 메가비트 한도를 설정하고 청구일을 사용자 지정해 사용량을 기준으로 알림을 생성할 수 있습니다. 이용할 수 있을 때 Wi-Fi를 사용해 혜택을 받도록 사용자에게 알려줄 것을 권장합니다. 자동 Wi-Fi 구성은 장치가 기업 내에 있는 동안 Wi-Fi에 자동 연결하도록 도움을 줍니다.

연금 계획이 50달러 또는 월별 데이터 사용량의 200 MB만 다룰 경우, 직원들은 제한 연령 초과를 책임지게 될 수도 있다는 경고를 받습니다.

9. 장치의 비준수 사항을 지속적으로 모니터링

장치가 등록되면, 이 모든 것은 컨텍스트에 대한 것입니다. 장치는 특정 시나리오를 지속적으로 모니터링해야 하며, 자동화된 정책을 제자리에 배치해야 합니다. 사용자가 관리를 비활성화하려 합니까? 장치가 보안 정책을 준수합니까? 보고 있는 데이터를 기준으로 조정해야 합니까? 여기서 생성해야 할 추가 정책이나 규칙에 대해 이해할 수 있습니다. 다음은 일반적인 몇 가지 예입니다.

- **탈옥의 "루트" 확보:** 직원은 종종 휴대폰을 "탈옥시키거나" "루팅하며", 정보를 도난당할 수 있는 악성 프로그램이 침입할 수 있는 입구를 개방합니다. 장치를 탈옥할 경우, MDM 솔루션은 장치에서 기업 데이터를 선택적으로 바로 삭제하는 등 조치를 취할 수 있어야 합니다.
- **삭제 전 여유 시간, SMS 보내기:** 앵그리 버드 비비기처럼 시간을 낭비하는 것은 기업 정책과 전혀 맞지 않습니다. 악의는 없습니다. 단지, 자동 지우기가 손이 많이 갈뿐입니다. MDM 솔루션은 공격을 기반으로 정책을 실행할 수 있습니다. MDM은 사용자에게 메시지를 전달할 수 있으며, IT가 지우기 버튼을 누르기 전 애플리케이션을 제거할 시간을 제공합니다.
- **새 운영 체제 이용 가능.** BYOD의 효력을 유지하기 위해, 사용자는 새 OS를 설치할 준비를 했을 때 알려주는 간편한 방법이 필요합니다. 올바른 MDM 솔루션을 활용해, OS 업그레이드는 셀프 서비스 기능이 됩니다. 이전 OS 버전의 제한은 규정 준수를 보장하도록 지원하며 장치 운영성을 최적화합니다.

10. BYOD로 인한 투자수익률 (ROI) 확보

BYOD는 구매 장치에 대한 책임을 직원에게 돌리면서, 조직을 위한 큰 그림을 그리고 장기간 비용을 고려할 가치가 있습니다.

정책을 집필하면서 그 정책이 ROI에 어떻게 영향을 미치는지 고려해보십시오. 이는 아래 나타난 바와 같은 비교 접근법을 포함합니다.

기업 소유 모델

- 각 장치에 들어가게 될 비용
- 전체 보조금 지급 데이터 계획 요금
- 매년 장치 재활용에 들어가는 비용
- 보증 계획
- 프로그램 관리 시 들어가는 IT 시간 및 노동력

BYOD

- 일부 보조금 지급 데이터 계획 요금
- 장치 구매 비용 제거
- 모바일 관리 플랫폼 비용

한 가지로 모든 것을 맞출 수는 없습니다. 하지만 잘 만들어진 BYOD 정책은 모바일 장치를 효과적이고 효율적으로 관리할 수 있는 방향을 제시합니다.

물론, 직원이 이동 중이고 항상 연결되어 있을 때 생산성이 향상됩니다. BYOD는 이전에 기업 장치에 적합하지 않았던 신규 사용자에게 이와 같은 생산성 향상이 가능하도록 제공하는 뛰어난 방법입니다.

BYOD: 자유의 보안

BYOD은 자체 장치로 작업할 수 있는 자유를 직원에게 부여하고 그와 동시에 IT의 중요한 재무 및 관리 부담을 완화하는 모범 사례로 등장했습니다. 그러나, BYOD는 서면 작성된 정책이나 견고한 관리 플랫폼 없이는 효율화된 관리 및 비용 절약이라는 약속을 지킬 수 없습니다.

아직 모바일 전략 초기 단계에 있을 경우, IBM® MaaS360® 은 풍부한 교육 자원을 제공합니다.

BYOD가 귀하의 비즈니스에 적합하다고 여기신다면 여기를 클릭해 MaaS360 무료 30일 시험판을 체험해 보십시오. MaaS360은 클라우드 기반이기 때문에 데이터 손실 없이 테스트 환경이 자동적으로 생산 환경으로 적용되게 됩니다.

IBM MaaS360 정보

IBM MaaS360은 엔터프라이즈 이동성 관리 플랫폼으로서 사람들의 업무 방식과 관련된 생산성 및 데이터 보호 기능을 제공합니다. MaaS360은 수천여 개의 조직들로부터 이동성 이니셔티브의 기반으로 인정받고 있습니다. MaaS360은 어떤 모바일 배포 과정이든 지원할 수 있도록 사용자, 장치, 앱 및 컨텐츠 측면에서 모두 강력한 보안 제어를 가능케 함으로써 종합적인 관리를 도와줍니다. IBM MaaS360에 대한 자세한 정보를 보고, 무료 30일 시험판을 시작하려면, 다음 웹페이지를 방문하십시오. www.ibm.com/maas360

IBM Security 정보

IBM의 보안 플랫폼은 조직에서 직원, 데이터, 애플리케이션 및 인프라를 총체적으로 보호할 수 있도록 도와주는 보안 인텔리전스를 제공합니다. IBM은 ID 및 액세스 관리, 보안 정보 및 이벤트 관리, 데이터베이스 보안, 애플리케이션 개발, 위험 관리, 엔드포인트 관리, 차세대 침입 보호 등을 위한 솔루션을 제시합니다. IBM은 전 세계 가장 광범위한 보안 연구 개발 및 인도 성과를 자랑하는 조직 중 하나입니다. 자세한 정보는 다음 웹사이트를 참조하십시오. www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
2016년 3월

WGW03112-KRKO-01