egloo

Enkel Säkerhetspolicy för Mobila enheter

egloo

Att använda denna policy

En av utmaningarna IT-avdelningar har i dag är att säkrar både privat- och företagsägda mobila enheter, såsom surfplattor och smarta telefoner. Denna policy är tänkt att fungera som riktlinje för organisationer som behöver implementera eller uppdatera en befintlig säkerhetspolicy för mobila enheter.

Känn dig fri att anpassa denna policy för att passa din organisations risktolerans och användarprofil. Om så krävs, justera, ta bort eller lägga till information för att anpassa policyn utefter din organisations behov. Detta är inte en heltäckande policy utan snarare en pragmatisk mall avsedda att tjäna som grund för din egen policy.

Bakgrunden till denna policy

Företagens IT-avdelningar står inför två utmaningar när de överväger en Mobilpolicy: en blandning av företags- och personalägda enheter har åtkomst till företagets nätverk och data, dessutom används dessa enheter för både professionella och personliga ändamål.

Med data som transporteras över publika nätverk, till och från enheter som är lätta att tappa eller stjäla, blir oro för dataskydd avgörande och den främsta drivkraften för att genomföra Mobile Device Management system och policys. Säkerheten måste stå i centrum för en organisations mobila strategi för att skydda företagsdata, upprätthålla efterlevnad, minska riskerna och garantera mobil säkerhet på alla enheter.

Denna policy ger ett ramverk för att säkra mobila enheter och bör kopplas till andra policyområden som stödjer organisationens IT och datasäkerhet.

Ett Bring-Your-Own-Device initiativ kan endast genomföras framgångsrikt om vissa säkerhetsprinciper efterlevs. En Mobile Device Management-lösning är en förutsättning för att genomföra detta.

egloo

Policy

1. Introduktion

Mobila enheter, såsom surfplattor och smarta telefoner, är viktiga verktyg för organisationen och **<Företag X>** stöder deras användning för att uppnå affärsmålen.

Mobila enheter utgör dock en betydande risk för datasäkerheten som, om lämpliga tillämpningar och säkerhetsförfaranden inte tillämpas, kan vara en kanal för obehörig åtkomst till organisationens data och IT-infrastruktur. Detta kan sedan leda till dataläckage och systeminfektion.

<Företags X> har ett krav på att skydda sina informationstillgångar för att skydda sina kunder, immateriella rätt och rykte. Detta dokument beskriver en uppsättning av metoder och krav för säker användning av mobila enheter och applikationer.

2. Omfattning

1. Alla mobila enheter, vare sig de ägs av **<Företag X>** eller ägs av den anställda, inklusive surfplattor och smarta telefoner, som har tillgång till företagets nätverk, data och system omfattas av denna mobila policy för enhetssäkerhet. Denna policy omfattar inte företagets IT förvaltade bärbara datorer.
2. Undantag: Om det finns ett affärsbehov som måste undantas från denna policy (alltför dyrt, alltför komplex, negativt påverkande andra affärskrav) måste godkännande av risken göras av säkerhetsansvarig.
3. Applikationer som används av anställda på sina egna personliga enheter som lagrar eller har tillgång företagsdata, t ex appar för molnlagring, är också föremål för denna policy.

3. Policy

3.1 Tekniska krav

1. Enheter måste använda följande operativsystem: Android 2.2 eller senare, iOS 4.x eller senare. **<lägga till eller ta bort vid behov>**
2. Produkterna skall lagra alla användarsparade lösenord krypterat.
3. Enheter måste konfigureras med ett säkert lösenord som uppfyller <Företag X> s lösenordspolicy. Detta lösenord får inte vara samma som alla andra lösenord som används inom organisationen.
4. Endast enheter som hanteras av IT kommer att tillåtas att ansluta till det interna företagsnätverket.
5. Dessa enheter kommer att omfattas av gällande regler och efterlevnad av säkerhetsfunktioner såsom kryptering, lösenord, nycklar, etc. Denna policy kommer att verkställas av IT-avdelningen med hjälp av Mobile Device Management mjukvara.

3.2 Användarkrav

1. Användarna får endast ladda företagsdata som är avgörande för deras roll på sin mobila enhet(er).
2. Användarna måste rapportera alla borttappade eller stulna enheter till **<Företag X>** IT omedelbart.
3. Om en användare misstänker att obehörig åtkomst till företagets data har skett via en mobil enhet, måste de rapportera incidenten i linje med **<Företag X>** 's incidenthanteringsprocess.
4. Produkterna skall inte vara "jailbreakade" eller "rootade" * eller ha någon programvara/firmware installerad som är utformad för att få tillgång till funktionalitet som inte är avsedda för användaren.
5. Användare får inte installera piratkopierad programvara eller olagligt innehåll på sina enheter.
6. Appar får endast installeras från officiella, av IT, godkända källor. Installation av kod från opålitliga källor är förbjudet. Om du är osäker på om en app är från en godkänd källa kontakt **<Företag X>** IT.
7. Produkterna skall hållas à jour med tillverkaren eller av IT tillhandahållna uppdateringar. Som ett minimum bör uppdateringar kontrolleras en gång i veckan och tillämpas minst en gång i månaden.
8. Enheter får inte vara anslutna till en dator som inte har ett uppdaterat och aktiverat anti-virus och som inte överensstämmer med företagets policy.
9. Produkterna skall vara krypterade i linje med **<Företag X>**'s efterlevnads standard.
10. Användare måste vara försiktig om både personliga och arbetsrelaterade e-postkonton installeras på sina enheter. De måste ta särskild omsorg för att säkerställa att företagets data endast sänds via företagets e-postsystem. Om en användare misstänker att företaget data har skickats från ett personligt e-postkonto, antingen i brödtexten eller en bifogad fil, måste de anmäla detta till **<Företag X>** IT omedelbart.
11. Ovanstående krav kommer att kontrolleras regelbundet och om en enhet inte är kompatibel kan det leda till förlust av tillgång till e-post, enheten låses, eller i särskilt svåra fall, att enheten raderas.
12. Användaren är ansvarig för säkerhetskopiering av sina egna personuppgifter. Företaget tar inte på sig något ansvar för förlust av personliga filer på grund av att en icke kompatibel enhet raderas av säkerhetsskäl.
13. (I förekommande fall för din organisation) Användare får inte använda företagets datorer för att säkerhetskopiera eller synkronisera personligt enhetsinnehåll såsom mediefiler, såvida inte ett sådant innehåll krävs för affärsändamål.

** Att jailbreaka/roota en mobil enhet är att ta bort de begränsningar som tillverkaren ålagt. Detta ger tillgång till operativsystemet, och låser därmed upp alla funktioner som möjliggör installation av otillåtna program.*

3.3 Åtgärder som kan leda till en fullständig eller delvis radering av enheten, eller annan åtgärd av IT

1. En enhet är jailbreakad/rootad
2. En enhet innehåller en app känd för att innehålla ett säkerhetsproblem (om den inte avlägsnas inom en given tidsram efter att IT har informerat användaren)
3. En enhet försvinner eller blir stulen
4. En användare har överskridit det maximala antalet misslyckade lösenordsförsök

3.4 Användning av speciella tillämpningar som har tillgång till företagets data

1. Lagringslösningar i molnet: **<Företag X>** stöder användning av följande lagringslösningar i molnet **xxxxxx**.
2. Användningen av andra än ovanstående lagringslösningar i molnet leder till ett brott av säkerheten och leder till förlust av tillgång till företagets nätverk för användaren.

Prata med oss om Mobile Control

BYOD är dagens verklighet. Om du anammar dessa enheter, ser du de produktivitetsvinster, ökad effektivitet, och innovationer de ger upphov till hos en rörlig organisation. Men du måste ha de rätta lösningarna på plats från början.

Vi hjälper dig att utvärdera och implementera Mobile Control. Det är enkelt och kostnadseffektivt att säkra användaren, deras mobila internet-access och företagets affärsdata.

Med per användare licensiering innebär det att du kan säga ja till BYOD utan att begränsa antalet eller typen av enheter dina slutanvändare har. Ta kontroll över mobil säkerhet med oss på Egloo.

För frågor och mer information, kontakta:

Kenneth Steinholtz
0735 – 19 71 14
erbjudande@egloo.se