UPPSALA UNIVERSITET

Dnr UFV 2018/1675

Säker hantering av mobila enheter och portabla lagringsmedia

Rutiner för informationssäkerhet

Fastställda av Säkerhetschefen 2018-09-03

Innehållsförteckning

1 Inledning

I allt högre utsträckning används olika typer av mobila enheter för hantering och lagring av information. Smarta mobiltelefoner, surfplattor och bärbara datorer har i mycket hög utsträckning kommit att ersätta utrustning som tidigare hade en fast placering i skyddade kontorsmiljöer. Därtill har användningen av portabla lagringsmedia i form av USB-minnen och externa hårddiskar öppnat för möjligheten att information, ibland känslig sådan, lagras på media som hanteras i mer öppna och oskyddade miljöer.

Nedanstående rutiner har fastställts i syfte att stödja en korrekt och säker hantering av mobila enheter – en användning som skyddar mot informationsförlust och andra tänkbara säkerhetsmässiga incidenter.

Rutinerna baseras på baseras på universitetets rutiner för informationssäkerhet (UFV 2017/93) och riktlinjer inom IT-området (UFV 2013/907, UFV 2016/896).

2 Ansvar

2.1 Efterlevnad

Ansvaret för efterlevnad av dessa rutiner fördelar sig enligt följande:

Prefekt/motsvarande vid sin institution, avdelning eller motsvarande.

Områdesföreståndare för samordning inom sitt intendenturområde.

Systemägare, e-områdesansvarig/motsvarande för att följa rutinerna i utvecklings- och förvaltningsarbete samt driftuppdrag. Ansvar för efterlevnad gäller även då annan intern eller extern part anlitas för uppdraget. Utförande parts ansvar ska i förekommande fall regleras i ett s.k. servicenivåavtal.

Säkerhetschef för planering, samordning och uppföljning samt kontroll av efterlevnad.

Verksamma vid universitetet för att följa rutinerna.

2.2 Uppdatering av rutinerna

Säkerhetschefen ansvarar för att rutinerna kontinuerligt uppdateras och att underliggande stöddokument fastställs.

3 Definitioner

Virtual private Network (VPN) är en teknik som används för att skapa en säker förbindelse eller "tunnel" mellan två punkter i ett icke-säkert nätverk. För medarbetare vid universitetet som har behov av att arbeta på distans eller ha tillgång till universitetets resurser under tjänsteresa finns möjlighet att via VPN-tjänsten ansluta säkert till universitetets nätverk.

Bluetooth/ Blåtand är en standard för trådlös kommunikation som möjliggör sammankoppling av olika typer av externa enheter och exempelvis en mobiltelefon.

Visual hacking innebär att en person visuellt inhämtar information, exempelvis genom att se vad som visas på en annan persons datorskärm.

Mobil enhet är här begränsat till mobila IT-enheter – d.v.s. bärbara datorer, mobiltelefoner (smartphones), surfplattor och liknande digitala apparater, samt externa lagringsenheter (portabla lagringsmedia) som externa hårddiskar och USB-minnen.

4 Omfattning

4.1 Från anskaffning till avveckling

En säker hantering av mobila enheter innehåller hela enhetens livscykel, från anskaffning (inköp) till avveckling.

Alla inköp ska hanteras enligt *riktlinjer för upphandling* (UFV 2010/1853) och bör om möjligt göras via universitetets produktwebb.

Klienthanteringssystem som (ibland med tilläggsmodul) även har stöd för hantering av mobila enheter (specifikt smart phones) används i stor utsträckning på universitetets campusområden. Mobila enheter som ansluts och administreras via klienthanteringssystem får automatiskt stöd med säkerhetsinställningar, säkerhetskopiering, kryptering, fjärrdeaktivering/-radering, antivirus med mera. Rekommendationen är att alla mobila enheter bör, om möjligt, anslutas till ett klienthanteringssystem.

För avveckling (utrangering) finns stöd i *rutiner för utrangerad utrustning* (UFV 2014/1279). Oavsett om utrustning ska flytta mellan användare inom en institution/motsvarande, mellan institutioner/motsvarande inom universitetet, avvecklas eller avyttras (kasseras, bytas bort eller försäljas) är det viktigt att förhindra obehörig åtkomst till informationen.

4.2 Skydd av mobil enhet

Utrustning ska förvaras säkert och hållas under uppsikt.

Mobila enheter ska skyddas med automatisk låsning/skärmsläckare och lösenord eller PIN-kod. Enheter som innehåller känslig information eller som används för access till sådan ska alltid ha denna funktion aktiverad.

Fysiskt datorlås bör användas då bärbar dator lämnas i öppna kontorsytor.

Sekretessfilter, som ger begränsad insyn till det som exponeras på skärmen, bör användas då bärbar dator används i öppna miljöer.

Bärbar dator ska skyddas med ett aktuellt och uppdaterat antivirusprogram. En rekommendation är att förse även smarta mobiltelefoner och surfplattor med ett sådant skydd.

Prefekt ska meddelas vid stöld eller annan förlust av enhet på institutionen.

4.3 Anslutning till publika nätverk

Stor försiktighet ska iakttas vid användning av publika nätverk. Öppna publika nätverk som inte skyddas av lösenord bör så långt det är möjligt undvikas. Nätverk som skyddas av lösenord som delas av många, exempelvis vid konferensanläggningar eller hotell, ska användas på ett sätt som minimerar risker:

- Ange aldrig lösenord eller annan känslig information via okrypterad förbindelse (http).
- Ge akt på certifikatsvarningar – fullfölj inte access till en webbplats vid erhållen varning om att problem med webbplatsens säkerhetscertifikat uppstått.
- Iaktta stor försiktighet vad gäller funktioner som tillåter delning av filer och skrivare samt fjärrinloggning.

Håll enhetens lista över kända trådlösa nätverk aktuell. Rensa listan från nätverk som du inte använder.

Om enhetens operativsystem möjliggör detta – stäng av funktionen för automatisk uppkoppling mot trådlöst nätverk.

Om åtkomst till system innehållande känslig information sker på distans ska universitetets VPN-tjänster för säker internetuppkoppling användas.

4.4 Användning av mobil enhet

Användning av appar

Installera bara appar du behöver och som levereras av betrodda källor. Godtycklig nedladdning och användning av appar ökar risken för att oseriös och skadlig programvara installeras på enheten.

Håll samtliga program och appar uppdaterade. Genom att använda aktuella programversioner kan risken för att enheten drabbas av skadlig kod minskas i väsentlig grad.

Var observant då appar begär tillgång till resurser på enheten. Många appar frågar efter tillgång till resurser som inte är relevanta i sammanhanget.

Vid användning av appar kan det vara svårt att veta om trafiken verkligen krypteras – använd endast appar som du litar på.

Portabla lagringsmedia

Portabla lagringsmedia är praktiska, men speciellt USB-minnen kan lätt tappas bort. Överväg lämpligheten med att lagra känslig information i sådana.

Information som lagras i portabla lagringsmedia, såsom USB-minnen och externa hårddiskar, bör krypteras.

Anslut inte USB-minnen med okänt innehåll till dina enheter. USB-minnen som delas ut gratis, exempelvis vid mässor eller konferenser, ska användas med stor försiktighet. Sådana kan innehålla skadlig kod som drabbar den enhet de ansluts till.

Övrig hantering

Öppna inte SMS/MMS eller e-post från okända avsändare och klicka inte på länkar som skickats från okända.

Avaktivera positionstjänster och bluetooth när de inte behövs. Sådana tjänster kan göra enheten synlig för aktörer med tveksamma syften och ökar därigenom risken för att den drabbas av skadlig kod.

4.5 Resesäkerhet för mobila enheter

En resa medför särskilda risker för den information och de enheter du tar med på resan. Nedanstående vägledning ger dig stöd i hanteringen inför, under och efter resan.

Före resan

- Information som på hemmaplan lagras i en lagringslösning med hög säkerhet kan utsättas för stora risker om du kopierar över den till en mobil enhet som du tar med dig på resan. Ta bara med dig den information du behöver på resan
- Användning av dina enheter utanför den ordinarie kontorsmiljön ökar risken för att förlora dem eller att de ska utsättas för någon form av angrepp. Ta bara med de enheter som du verkligen behöver
- Se till att du har tillgång till universitetets VPN-tjänst. Om du inte redan har det - se instruktioner i Medarbetarportalen som visar hur du får tillgång till dessa
- Uppdatera programvaran på dina enheter
- Se till att dina enheter är utrustade/konfigurerade med standardmässigt säkerhetsskydd (automatisk låsning, lösenord/PIN-kod, uppdaterat antivirusprogram etc.)
- Uppdatera dig på aktuell information om landet som är föremål för din resa. Finns särskilda regler vad gäller att medföra krypterad information? Finns andra regler/restriktioner? Undersök med resebyrån, UD och andra som besökt landet ifråga.

Under resan

- Håll ständig koll på dina enheter
- Om du använder din laptop i offentliga miljöer – se upp med visual hacking. Använd sekretessfilter på din skärm!
- Undvik att koppla upp dina enheter mot publika WiFi-nät. Du delar dessa nät med okända, en del med tveksamma syften. Vissa nät sätts upp specifikt för att stjäla uppgifter och sprida skadlig kod
- Även anslutning till lösenordsskyddade nätverk, exempelvis på hotell, kan medföra stora risker. Var kritiskt inställd till frågor som ställs i samband med anslutning till nätverket. Finns tillgång till Eduroam utgör det ett bra alternativ. Universitetets VPN-tjänster ger krypterad kommunikation till dina resurser vid universitetet.
- Avaktivera tjänster som du inte behöver under resan (det kan exempelvis handla om positionstjänster och bluetooth).
- Om det delas ut gratis USB-minnen på mässan – undvik dessa och köp de du har behov av.
- Använd din egen laddare. På vissa hotell kan laddare finnas utplacerade i rummen, ibland riggade för att plantera skadlig kod i de enheter som ansluts.

Efter resan

- Kör en viruskoll på de enheter du haft med dig på resan
- Om du haft USB-minen med dig som använts under resan bör även dessa kontrolleras.
- Var särskilt uppmärksam på eventuella phishing-försök som kan ha koppling till din utlandsvistelse.