Universitair Informatiemanagement UNIVERSITEIT TWENTE.

Kenmerk: SB/UIM/12/1018/khv
Datum: 9 december 2013

Gebruik van “eigen” apparatuur en applicaties
Consequenties voor de UT-werkplek

Inhoud

Inhoud **1**

Samenvatting **2**

Rationale 2

Implicaties 2

Inleiding **3**

Algemeen **3**

Kosten en vergoedingen **3**

Ondersteuning **4**

Aanschaf 4

Apparatuur 5

UT-Applicaties **5**

Onderwijs **5**

Onderzoek **6**

Informatiebeveiliging **6**

Samenvatting

De UT-werkplek is gebaseerd op bring/choose-your-own-device (BYOD/CYOD), waarmee flexibel werken op en buiten de campus mogelijk is.

De i-Strategie UT 2014-2017 formuleert dit op hoofdlijnen als volgt, welke tekst prima als samenvatting van dit beleidsstuk kan functioneren.

Rationale

Het gebruik van een grote diversiteit aan mobiele devices neemt een grote vlucht: smart phones, tablets, ultrabooks, notebooks. Verschillende soorten en types devices volgen elkaar steeds sneller op. Deze devices zijn zelf aangeschaft (BYOD), of bekostigd door de UT (CYOD). Beide varianten duiden we aan met BYOD. Het voorschrijven van bepaalde devices is met deze snelle ontwikkelingen in een gemeenschap van professionals niet wenselijk. Creativiteit en state-of-the-art gebruik van ICT zouden daardoor onnodig beperkt worden.

Mobiele toegang tot informatie- en ICT-diensten is zeer gewenst. Studenten en medewerkers zijn meer en meer mobiel, en verwachten daarbij onderweg goede toegang tot informatie- en ICT-diensten. Omgekeerd verwacht de UT-organisatie (en derden) ook dat medewerkers altijd goed bereikbaar zijn, ongeacht waar ze zich bevinden. Het meer in zwang raken van Het Nieuwe Werken draagt forst bij aan de wens om mobiele toegang met eigen devices tot informatie- en ICT-diensten.

Implicaties

De UT faciliteert het gebruik van eigen gekozen devices. De UT stelt beleid vast, waarin de kaders voor gebruik, ondersteuning en bekostiging van BYOD afgesproken worden.

De UT houdt een lijst van voorkeursdevices bij, waarover bij de ondersteuning diepgaander kennis aanwezig is. Voor andere devices is de gebruiker afhankelijk van per type device en/of operating system online beschikbaar gestelde handleidingen.

Informatie- en ICT-diensten van de UT zijn zoveel mogelijk toegankelijk via open standaarden, waardoor er zo min mogelijk afhankelijkheid van bepaalde typen devices is.

De UT informeert medewerkers en studenten over de risico's van privacy en security met mobiele devices. Niet alle risico's kunnen met technische maatregelen bestreden worden. Veel is ook afhankelijk van bewustwording en gedrag van medewerkers en studenten, die daarin hun eigen verantwoordelijkheid moeten nemen.

Dit beleidsdocument is onder meer kaderstellend voor een in 2014 door ICTS te starten project BYOD. In dat project zal de technische en praktische uitvoerbaarheid worden meegenomen in de nog te maken keuzes voor de inrichting van de dienstverlening rond BYOD. Een deel van de dienstverlening door ICTS zoals beschreven in de notitie kan pas geleverd worden nadat dat project zijn resultaat heeft opgeleverd. Hierover zal in de loop van 2014 door ICTS nader worden gecommuniceerd.

Inleiding

De laatste jaren is er een trend op de UT waar te nemen waarbij medewerkers en studenten meer en meer eigen keuzes maken ten aanzien van apparatuur, applicaties en clouddiensten. Daarbij komen vragen op rondom de gewenste ondersteuning en de noodzakelijke beveiliging.

Deze trend wordt vaak beschreven als Bring/Choose Your Own Device (BYOD/CYOD), als Consumerization of IT (CoIT), Bring Your Own Computer (BYOC) of als Use your own. Ook Het Nieuwe Werken gaat uit van locatie en tijd onafhankelijk werken, o.a. met privé-computers. De consequenties voor de UT worden geformuleerd in dit beleid. Er zijn raakvlakken met het Softwarelicentiebeleid, het Informatiebeveiligingsbeleid, de sourcingstrategie en het arbobeleid.

De UT-werkplek is gebaseerd op bring/choose-your-own-device (BYOD/CYOD), waarmee flexibel werken op en buiten de campus mogelijk is.

Algemeen

1. Er is een standaard werkplek (laptop, desktop) beschikbaar, beheerd door ICTS, welke voor het gros van de medewerkers uitstekend geschikt is als normale werkplek. Wanneer in gelijke gevallen gelijke keuzes worden gemaakt (standaardisatie) dan is dat voor de UT als geheel efficiënter en goedkoper.
2. Overwegingen om andere apparatuur te gebruiken zijn het elders, thuis of onderweg werken. Verder is afhankelijk van de toepassing en persoonlijke voorkeur het ene apparaat, applicatie of clouddienst meer geschikt of productiever dan het andere.
3. De UT legt de verantwoordelijkheid voor de keuze welke apparatuur en applicaties te gebruiken bij de individuele medewerker. Om de consequenties te overzien kan hij gebruik maken van de aanwezige deskundigheid bij ICTS, Inkoop en HR. Randvoorwaarden ten aanzien van deze keuzes worden geformuleerd in dit beleid.
4. De keuzevrijheid en bijbehorende individuele verantwoordelijkheid om af te wijken van de standaard en meer of andere apparatuur en applicaties te gebruiken wordt gefaciliteerd zoals beschreven in dit beleid. Hierbij worden randvoorwaarden vanuit verschillende oogpunten geformuleerd.
5. Ten aanzien van de aanschaf van apparatuur gelden verplichtingen volgend uit Europese aanbestedingen. Alleen met goede redenen kan hiervan worden afgeweken.
6. De UT accepteert als gegeven dat door het gebruik van mobiele en/of privé-apparatuur het werk zich meer vermengt met het privéleven van de medewerker. Wanneer werknemers dat niet willen, dan kunnen zij (wanneer de functie dat toestaat) er voor kiezen om UT-apparatuur buiten werktijd uit te zetten.
7. Het werken met andere apparatuur of op andere tijden en locaties kan risico's met zich meebrengen voor de arbeidsomstandigheden. Leidinggevenden en medewerkers kunnen dit bespreken in de jaargesprekken en worden door HR ondersteund middels informatie op de HR website en de inspanning van de Arbo-coördinatoren.

Kosten en vergoedingen

8. De UT vergoedt geen privé-aanschaf van apparatuur, applicaties en clouddiensten of schade welke door werkgerelateerd gebruik aan privéapparatuur wordt veroorzaakt.
9. Eenheden kunnen er voor kiezen om (een deel van) de kosten van werkgerelateerde apps te vergoeden, ook als de medewerker privé-apparatuur gebruikt.

10. Door de belastingdienst wordt de verstrekking van devices (zoals een iPad en laptop) aangemerkt als loon, tenzij het zakelijk gebruik aantoonbaar meer is dan 90%.[1] Voor de smartphone en het mobiele telefoontoestel geldt de regel van minstens 10% zakelijk gebruik.
11. Of mobiele devices aan de betrokken medewerker ter beschikking worden gesteld, is een afweging van de betreffende eenheid. Er dient daarbij een standaard UT bruikleen-overeenkomst te worden gesloten. In deze overeenkomst worden ook eventuele (financiële) randvoorwaarden vastgelegd.

Ondersteuning

12. Gebruikers krijgen ondersteuning bij selectie, configuratie, storingen etc. van apparatuur, applicaties en clouddiensten. Niet alle gebruikerswensen en apparaten kunnen hierbij worden gefaciliteerd. Hieronder wordt per onderwerp verder uitgewerkt hoe en in hoeverre ondersteuning wordt geleverd.
13. Ondersteuning wordt (voor zover het apparaat dat mogelijk maakt) ten minste geleverd voor:
    a. het gebruik kunnen maken van het vaste en draadloze netwerk (UT-Net) en van VPN.
    b. de mogelijkheid om (via een beveiligde verbinding) e-mail op (mobiele) apparatuur te kunnen lezen en versturen en hun agenda te kunnen synchroniseren.
    c. de mogelijkheid om (via een beveiligde verbinding) documenten op (mobiele) apparatuur te kunnen lezen en bewerken. Er wordt uitgelegd hoe gebruikersdata (bijvoorbeeld op netwerkschijven) te benaderen is, welke software het meest geschikt is voor verschillende doeleinden en welke technische beperkingen er zijn.
    d. de mogelijkheid om documenten vanaf (mobiele) apparatuur te kunnen afdrukken. Er wordt uitgelegd welke apparatuur dit ondersteunt.
    e. het met Unified Communications (telefonie, messaging, data, etc.) kunnen communiceren op (mobiele) apparatuur. Er wordt uitgelegd welke apparatuur dit in hoeverre ondersteunt.
    f. het instellen van een backup en hoe deze terug te zetten.
14. Ondersteuning wordt geleverd via handleidingen op de website van ICTS. Voor de apparatuur waarvoor actieve ondersteuning wordt geleverd, zie punt 22, kunnen medewerkers voor ondersteuning terecht bij de servicedesk.

Aanschaf

15. Gebruikers krijgen ondersteuning bij de selectie van apparatuur (tablets, smartphones, laptops, USB-sticks, externe harde schijven etc.), applicaties (software) en clouddiensten (dataopslag, datatransfer, samenwerking, opslag en afspelen van video en presentaties, etc.). Deze ondersteuning wordt geleverd middels handleidingen op de website van ICTS, waar voor- en nadelen van de belangrijkste alternatieven worden gepresenteerd. Middels dit advies wordt onder meer gestimuleerd dat in gelijke gevallen gelijke keuzes worden gemaakt. Voor ondersteuning kunnen medewerkers ook terecht bij de servicedesk.
16. Daarnaast geeft de onderwijskundige dienst via haar website voorlichting over welke apparatuur, applicaties en clouddiensten hoe zinvol in het onderwijs zijn in te zetten.
17. Apparatuur, applicaties en clouddiensten worden ingekocht via de UT en ter beschikking gesteld aan de betrokken werknemer en blijft eigendom van de UT. Van de meest gekozen apparaten en onderdelen is een (kleine) voorraad aanwezig, dit wordt verder afgestemd in het kwartaaloverleg ICT & Onderzoek & Bedrijfsvoering. Voor de aanschaf van software wordt verwezen naar het Softwarelicentiebeleid.[2]

[1] De Belastingdienst stelt zich tot nu toe op het standpunt dat een iPad geschikt is voor privé doeleinden en dat 90% zakelijk gebruik moeilijk aantoonbaar is. Verwacht wordt dat bij een nadere vaststelling van de werkkostenregeling (ingangsdatum 1 januari 2015 bij de UT) de Belastingdienst dit standpunt zal bijstellen.
[2] Softwarelicenties en de UT, kenmerk SB/UIM/12/0601/khv, is op 12 maart 2013 in de UCB geaccordeerd, www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/softwarelicenties-en-de-ut.pdf

18. Medewerkers dragen er zorg voor alleen software met geldige licentie te installeren.
19. Medewerkers kunnen er voor kiezen om privé-aankopen voor UT-doeleinden te gebruiken, dit brengt geen verplichtingen voor de UT met zich mee.
20. Bij veel appstores voor tablets, smartphones en andere devices kan de aanschaf van applicaties niet via Inkoop van de UT geregeld worden en zal de medewerker dat dus zelf moeten doen. Eenheden wordt aangeraden om voor de vergoeding van de kosten van deze applicaties met normbedragen voor een set van geadviseerde apps te werken.

Apparatuur

21. Gebruikers krijgen ondersteuning bij de installatie en bij storingen van apparatuur. Deze ondersteuning wordt voor de meest gebruikte apparatuur geleverd middels handleidingen op de website van ICTS, waar de belangrijkste aspecten worden toegelicht.
22. Voor een beperkte set apparatuur en operating systemen wordt deskundige actieve ondersteuning via de servicedesk geleverd. Op de ICTS-website staat vermeld voor welke apparatuur deze actieve ondersteuning wordt geleverd.
23. Bij de ondersteuning wordt geen onderscheid gemaakt op grond van het feit of de apparatuur eigendom is van de UT of van de betrokken gebruiker.
24. Bij defecte (onderdelen van) privé-apparatuur wordt de gebruiker voor reparatie en garantie verwezen naar zijn leverancier.

UT-Applicaties

25. Voor het gebruik van webapplicaties die gebruikt worden in de backoffice van diverse administratieve processen wordt er vanuit gegaan dat de medewerker beschikt over een beheerde standaard werkplek. Dit betreft bijvoorbeeld het gebruik van Oracle Applications door medewerkers van FEZ en HR en het gebruik van Osiris door BOZ's. Gebruik van een bepaalde webbrowser en specifieke plug-ins kan hierbij noodzakelijk zijn. Wanneer andere apparatuur hiermee niet compatibel is dan kan deze niet gebruikt worden voor dit doel.
26. Voor het gebruik van webapplicaties die deel uitmaken van de frontoffice van diverse administratieve processen zijn open standaarden het uitgangspunt. Dit betekent dat de gebruiker ervan mag uitgaan dat de webapplicaties werken met zijn apparaat en browser.[3] Voorbeelden van frontoffice toepassingen zijn het gebruik van Osiris self-service door studenten en docenten en het gebruik van de studenten- en de medewerkersportal. De gebruiker kan zelf bepalen welke apparatuur en browser hij gebruikt om met de webapplicatie te werken, zonder dat plug-ins hierbij noodzakelijk zijn. ICTS stelt een plan op hoe dit gerealiseerd kan worden.
27. De UT gaat geen apps voor specifieke merkgebonden apparatuur ontwikkelen. Om studenten en anderen te faciliteren dergelijke apps te ontwikkelen wordt een standaard programmeerinterface (REST API – waar de UT webapplicaties bij voorkeur ook gebruik van maken) beschikbaar gesteld. ICTS stelt een plan op hoe dit gerealiseerd kan worden.

Onderwijs

28. Als een opleiding eisen stelt aan de hardware of software waar studenten over moeten kunnen beschikken, dan wordt dit ruim van te voren aan de studenten meegedeeld op soortgelijke manier als ook over het aanschaffen van boeken wordt gecommuniceerd.
29. Als een soort van virtuele PC-zaal kan de UT applicaties ter beschikking stellen ongeacht het operating systeem en capaciteit van de apparatuur van de student. ICTS levert deze dienst als maatwerk aan opleidingen.

[3] De implementatie van html5 door webbrowsers verschilt nog steeds, incidenteel kunnen er dus problemen optreden.

30. Docenten wensen ondersteuning bij de selectie en toepassing van moderne tools en technieken binnen het onderwijs. De onderwijskundige dienst speelt hier op in.
31. Per onderwijsruimte is het voor de docent duidelijk welke aansluitingen er beschikbaar zijn om gebruik te maken van de aanwezige apparatuur als beamer, digibord, etc.

Onderzoek

32. Ieder onderzoeksproject maakt met betrekking tot te gebruiken apparatuur eigen keuzes, hiervoor zijn geen aanvullende algemene richtlijnen te geven. ICTS kan daarbij adviseren.

Informatiebeveiliging

33. Zoals beschreven in het Informatiebeveiligingsbeleid[4] is informatiebeveiliging een lijnverantwoordelijkheid en ieders verantwoordelijkheid.
34. Afhankelijk van de classificatie van de informatie[5] kan beoordeeld worden of het verantwoord is dat informatie de UT verlaat en wat voor beveiligingsmaatregelen als versleuteling, screenlocks en de mogelijkheid van op afstand wissen noodzakelijk zijn. De UT zal niet standaard voor alle apparatuur deze beveiligingsmaatregelen implementeren. ICTS ontwikkelt hiervoor dienstverlening welke zo mogelijk via een selfservice webapplicatie wordt aangeboden.
35. De gebruiker is verantwoordelijk om te voorkomen dat er malware (virussen etc.) op het apparaat actief wordt. Wanneer een besmetting op het netwerk wordt gedetecteerd dan wordt het apparaat geïsoleerd tot het probleem is verholpen. Via de website van ICTS wordt voorlichting gegeven hoe besmetting te voorkomen en te verhelpen. Daarnaast wordt via de servicedesk actieve ondersteuning geleverd.
36. Mobiele apparatuur is gevoeliger voor beschadiging, diefstal en uitval dan desktop-apparatuur. Beschikbaarheid van de gegevens is een aandachtspunt dat door tijdige back-ups geregeld kan worden. Integriteit en Vertrouwelijkheid van de gegevens zijn een aandachtspunt, zeker als ook familie, vrienden of kinderen van de apparatuur gebruik kunnen maken. De gebruiker is zelf verantwoordelijk en wordt door ICTS en de direct leidinggevende op deze risico's gewezen. Hierbij wordt ook verwezen naar de nog te ontwikkelen algemene integriteitscode voor de gehele UT, die beschrijft wat de ethische waarden zijn die wij voorstaan en waarop men ons mag aanspreken.
37. ICTS plaatst op de website een richtlijn die ingaat op deze risico's, de mogelijkheden van preventie zoals het toepassen van versleuteling en het gebruik van wachtwoorden en beschrijft wat te doen wanneer apparatuur wordt gestolen of zoekraakt. Hierbij wordt o.a. aandacht besteed aan het zo snel mogelijk wijzigen van wachtwoorden opdat niet meer informatie gecompromitteerd kan worden doordat deze wachtwoorden op de apparatuur zijn ingesteld.
38. Niet voor alle soorten gegevens is het verantwoord dat deze de UT verlaat. Dit kan zowel betrekking hebben op gegevens opgeslagen in apparatuur als op clouddiensten. Gebruikers hebben behoefte aan een checklijst aan de hand waarvan zij kunnen beoordelen wat de risico's zijn. Universitair Informatiemanagement zal deze checklijst in samenspraak met ICTS ontwikkelen en via de website van ICTS beschikbaar stellen.
39. Bij de beveiliging van het UT-netwerk wordt er door ICTS rekening mee gehouden dat de gebruikte apparatuur niet gegarandeerd vrij is van malware.
40. Bij de beveiliging van applicaties wordt er door ICTS rekening mee gehouden dat het netwerk tussen het apparaat en de webserver niet vertrouwd is. Vertrouwelijke informatie wordt via een versleutelde verbinding verstuurd.

---

[4] Informatiebeveiligingsbeleid Universiteit Twente, SECR/UIM/11/0405/khv www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/informatiebeveiligingsbeleid.pdf
[5] Classificatierichtlijn Informatie en Informatiesystemen Universiteit Twente, SECR/IM/11/0412/khv www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/classificatierichtlijn-ut.pdf