Universiteit Stellenbosch: Voorskrifte oor Wagwoorde

1. Oorsig

Wagwoorde is ‘n belangrike aspek van rekenaarsekuriteit. Dit is die eerste verdedigingslinie vir gebruikersrekeninge. ‘n Wagwoord wat swak gekies is kan die Universiteit se hele netwerk in die gedrang bring. Gevolglik het alle werknemers van die Universiteit (kontrakteurs en verskaffers met toegang tot die Universiteit se stelsels ingesluit) en studente die verantwoordelikheid om gepaste stappe, soos hieronder uiteengesit, te neem om hulle wagwoorde te kies en te beveilig. Die Elektroniese Kommunikasiebeleid (EKB) plaas ook die volgende verantwoordelikheid t.o.v. wagwoorde op die gebruiker: om wagwoorde vertroulik te hou en dit met niemand te deel nie.

2. Doel

Die doel van hierdie voorskrifte is om **vereistes** en **riglyne** neer te lê vir die skep van goeie wagwoorde, vir die beskerming van hierdie wagwoorde en vir die gereelde wysiging daarvan.

3. Omvang

Hierdie voorskrifte is aanvullend tot die Universiteit se Regulasies oor Informasiesekuriteit (I-Sek) en moet in konteks van laasgenoemde gelees word. Dit is van toepassing op alle personeellede en studente wat ‘n rekening het, of verantwoordelik is vir een, (of enige vorm van toegang wat ‘n wagwoord ondersteun of vereis) op enige stelsel wat in enige Universiteitsfasiliteit aangetref word, wat toegang tot die Universiteitsnetwerk het of wat enige nie-openbare Universiteitsinligting stoor.

Alle wagwoorde moet aan die onderstaande **vereistes** voldoen en moet verkieslik die onderstaande **riglyne** volg. (Sien die definisies van vereistes, riglyne en beleid in 9).

4. Riglyne en Vereistes

4.1. Stelselvlak en Gebruikersvlak: vereistes vir gereeldheid-van-wagwoordwysiging

4.1.1. Alle **stelselvlakwagwoorde** (bv. *root*, *enable*, NT-admin, programadministrasierekeninge, ens.) moet afsonderlik in verseëlde koeverte gestoor en in brandkluise in die IT-rekenaarkamer en die Rampherstel-rekenaarkamer geplaas word.

4.1.1.1. Hierdie wagwoorde sal normaalweg nie deur stelseladministrateurs gebruik word nie.

4.1.1.2. As die koevertseël egter gebreek word, moet die wagwoord gewysig en in die koevert teruggeplaas en verseël word.

4.1.1.3. Indien die wagwoord uit die koevert gehaal is deur iemand wat nie ‘n stelseladministrateur is nie, word die geval as ‘n sekuriteitsinsident geklassifiseer en moet die bepaalde stelseladministrateur ingelig en die wagwoord gewysig word.

4.1.1.4. Waar moontlik, behoort die gebruik van sodanige wagwoord stelselmatig beperk te word tot ‘n netwerksegment of stelselkonsole.

4.1.2. Alle **gebruikersvlakwagwoorde** (bv. Outlook, Webmail, Novell Netware, WebCT, portaal, tafelrekenaar, ens.) moet minstens elke 3 maande gewysig word. Sien ook riglyne vir Enkelaanmeldings (SSO’s) in 5.

4.1.3. ‘n Spesiale soort gebruikersvlakwagwoord sluit die wagwoorde in wat stelseladministrateurs gebruik om rekenaarstelsels mee te administreer. Dit is nie die stelselvlakwagwoorde waarna in 4.1.1 verwys is nie. Die vereiste soos in 4.1.2 beskryf is van toepassing, buiten dat die SSO-wagwoord nie gebruik moet word nie.

4.2. Algemene Riglyne vir Wagwoordopstelling

4.2.1. Die Universiteit gebruik wagwoorde in verskeie gevalle. Van die meer algemene gebruike daarvan sluit in: Windows-rekeninge, Novell druk- en lêerdiensterekeninge, portaalrekeninge, WebCT-rekeninge, administratiewe stelselrekeninge, e-posrekeninge, skermskutbeveiliging, ens. Aangesien baie min stelsels ondersteuning bied vir eenmalige gevalle (m.a.w. dinamiese wagwoorde wat net een keer gebruik word), <u>moet almal weet hoe om goeie wagwoorde te kies</u>. Wagwoorde moet maklik wees om te onthou, maar moeilik om te raai.

4.2.2. **Swak wagwoorde** beskik oor die volgende eienskappe:

- 4.2.2.1. Die wagwoord bevat minder as agt (8) karakters.
- 4.2.2.2. Die wagwoord is ‘n woord wat in woordeboeke voorkom.
- 4.2.2.3. Die wagwoord is ‘n alledaagse gebruikswoord soos:
  - 4.2.2.3.1. Name van gesinslede, troeteldiere, medewerknemers, fantasiekarakters;
  - 4.2.2.3.2. Rekenaarterme en -name, bevele, webwerwe, maatskappye, apparatuur, programmatuur;
  - 4.2.2.3.3. Die woorde "universiteit", "stellenbosch", "stell", "US" of enige afleiding daarvan;
  - 4.2.2.3.4. Verjaarsdae en ander persoonlike inligting soos adresse en telefoonnommers;
  - 4.2.2.3.5. Woord- of nommerpatrone soos aaabbb, qwerty, 123qwe, zyxwvuts, 123321, ens.;
  - 4.2.2.3.6. Enige van bogenoemde agterstevoor gespel;
  - 4.2.2.3.7. Enige van bogenoemde deur ‘n syfer voorafgegaan of gevolg (bv. geheim1, 1geheim).

4.2.3. **Goeie wagwoorde** beskik oor die volgende eienskappe:

- 4.2.3.1. Bevat beide hoof- en kleinletters (bv. a-z, A-Z)[1].
- 4.2.3.2. Bevat syfers en punktuasietekens, bv. 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
- 4.2.3.3. Kan spasies bevat, buiten aan die einde van wagwoorde.
- 4.2.3.4. Dit is minstens agt (8)[2], maar nie langer nie as twee-en-dertig (32), alfanumeriese karakters lank.
- 4.2.3.5. Dit is nie woorde in enige taal, sleng, dialek of jargon nie.
- 4.2.3.6. Dit is nie gebaseer op persoonlike inligting soos name van gesinslede nie.
- 4.2.3.7. Probeer goeie wagwoorde skep wat **maklik onthou kan word**. Een manier om dit te doen, is om ‘n wagwoord te skep wat op die titel van ‘n liedjie, ‘n verklaring of ander **frase** gebaseer is. Die frase kan bv. wees: "Ek het BComm by Maties geswot van 1991 tot 1993" en die wagwoord dan: "ehBCg@Mv91~93" of enige soortgelyke variasie. LET OP: Moenie enige van hierdie voorbeelde as wagwoorde gebruik nie!

4.3. Vereistes vir Wagwoordbeveiliging

4.3.1. Moenie die wagwoord wat jy vir Universiteitsrekeninge gebruik vir ander nie-universiteitsake (bv. persoonlike e-posrekening, internetbankdienste, mediesefondse, ens.) gebruik nie.

---

[1] Nie alle stelsels onderskei tussen hoof-en kleinletters nie;dit kan dus nie as 'n goeie sekuriteitsmaatreël beskou word nie.

[2] Verkieslik behoort wagwoorde uit 8 of meer karakters te bestaan, maar sommige stelsels het beperkings van slegs 6.

4.3.2. Kies afsonderlike wagwoorde vir die administratiewe stelsels (die "groen skerms"), ftp-en telnetrekeninge en 'n SSO-wagwoord vir ander IT-stelsels.
4.3.3. U vorige 10 wagwoorde op Universiteitstelsels kan nie weer gebruik word nie.
4.3.4. Moenie die Universiteitswagwoorde met enigiemand deel nie, administratiewe assistente en sekretaresses ingesluit. Alle wagwoorde moet as sensitiewe en vertroulike universiteitsinligting hanteer word.
4.3.5. Hier is 'n lys "moenies":
4.3.5.1. Moenie 'n wagwoord aan ENIGIEMAND oor die telefoon bekendmaak nie;
4.3.5.2. Moenie 'n wagwoord aan jou hoof bekendmaak nie;
4.3.5.3. Moenie voor ander mense oor 'n wagwoord praat nie;
4.3.5.4. Moenie leidrade gee oor die formaat van 'n wagwoord nie (bv. "my van");
4.3.5.5. Moenie 'n wagwoord op vraelyste of sekuriteitsvorms bekendmaak nie;
4.3.5.6. Moenie 'n wagwoord met gesinslede deel nie;
4.3.5.7. Moenie 'n wagwoord aan mede-werknemers bekendmaak tydens vakansie nie.
4.3.6. Wagwoorde moenie ingesluit word in e-posboodskappe of enige ander vorm van elektroniese kommunikasie nie.
4.3.7. Indien iemand aandring op u wagwoord, verwys hulle na hierdie dokument of laat hulle Informasietegnologie (IT) se hulpkantoor skakel.
4.3.8. Moenie die "Remember Password"-opsie van programme (bv. Internet Explorer, Outlook, Netscape Messenger) gebruik nie.
4.3.9. Weereens, moenie wagwoorde neerskryf en dit êrens in u kantoor bêre nie.
4.3.10. Moenie wagwoorde in 'n lêer stoor op ENIGE rekenaarstelsel (bv. persoonlike sakrekenaars, *smartphones* of soortgelyke toestelle) sonder enkripsie nie.
4.3.11. Indien die vermoede bestaan dat 'n rekening of wagwoord gekraak is, meld die insident by die IT-hulpkantoor aan en wysig alle wagwoorde.
4.3.12. Informasietegnologie of van hulle afgevaardigdes kan op 'n gereelde basis wagwoorde probeer kraak of raai. Indien 'n wagwoord tydens een van hierdie skanderings bekend word, sal die gebruiker versoek word om die wagwoord te wysig.

5. Riglyne vir Enkelaanteken (*Single sign-on - SSO*)

5.1. Gebruikers word aangemoedig om al hulle gebruikersvlakwagwoorde (Novell network, Outlook/Webmail, Internet/Inetkey) as *dieselfde wagwoord* te stel deur die wagwoordsinkroniseringsfunksie te gebruik. Hierdie wagwoord word ook vir .portale (mymaties.com, my.sun.ac.za en matiesalumni.net) en toegang tot Sun-e-HR en WebCT gebruik.
5.2. Die beginsel hier is dat indien gebruikers minder wagwoorde hoef te onthou, hulle beter wagwoorde sal kies en dit nie op logiese plekke sal stoor waar dit maklik gevind kan word nie.
5.3. Kies egter 'n *afsonderlike wagwoord* vir die administratiewe stelsels (die "groen skerms ").

6. Vereistes vir Herwinning en Wysiging van Wagwoorde

6.1. Personeel
6.1.1. Vir die administratiewe stelsel ("groenskerms") se wagwoorde: kontak die stelsel se wagwoordadministrateur en vra 'n wagwoordherwinnig of -wysiging aan.
6.1.2. Vir alle ander wagwoorde moet personeellede die bestuurder van die betrokke fakulteit se rekenaargebruikersarea (RGA) of die IT-hulpkantoor skakel of e-pos. Die opsie wat verkies word, is om die selfhelpfasiliteit te gebruik; die tweede opsie is om die personeellid se identiteit interaktief te bevestig deur 'n aantal persoonlike vrae te beantwoord. Indien dit misluk, moet die personeellid persoonlik aanmeld met bewys van identiteit.
6.2. Studente moet by die hulplyn van hulle rekenaargebruikersarea (RGA) aanmeld met bewys van identiteit (studentekaart, identiteitsdokument of paspoort).

6.3. Studente wat afstandsonderrig ontvang (of buite-kampuspersoneellede) moet die selfhelpfasiliteit gebruik, of indien dit misluk, hulle fakulteit se RGA-bestuurder of die IT-hulpkantoor skakel of e-pos. Hulle identiteit sal interaktief bevestig word deur 'n aantal persoonlike vrae te beantwoord. Studentenommers en 'n identiteits- of paspoortnommer moet by die e-pos ingesluit word.

6.4. Alle versoeke en wysigings, datum, tyd, gebruiker wie se wagwoord gewysig is, persoon wat die verandering gefasiliteer het en die IP-adres waarvandaan die versoek gerig is, sal aangeteken word.

7. Vereistes vir Programontwikkeling

Programmeerders moet seker maak dat hulle programme die volgende veiligheidsmaatreëls bevat:

7.1. Dit moet die verifikasie van individuele gebruikers ondersteun; nie van groepe nie.

7.2. Dit moenie wagwoorde in duidelike teks of enige ander omkeerbare vorm stoor nie.

7.3. Dit moet nooit 'n ongeënkripteerde wagwoord bo-oor 'n netwerkaansluiting dra nie.

7.4. Dit moet voorsiening maak vir rol-gebaseerde toegangsbeheer sodat een gebruiker die ander een se funksies kan oorneem sonder dat dit nodig is om daardie wagwoord te ken.

7.5. Dit moet beveiligde LDAP- of RADIUS-verifikasie soos relevant ondersteun, waar ookal nodig.

8. Handhawing

Indien enige gebruiker versuim om hierdie voorskrifte na te kom, sal hy/sy die gevolge dra soos in die Beleid oor Elektroniese Kommunikasie uiteengesit.

9. Definisies

Terme	**Definisies**
Riglyne	Tipies 'n versameling stelsel- of prosesspesifieke "voorstelle" vir optimale gebruik. Dit is nie voorwaardes wat nagekom moet word nie, maar word wel sterk aanbeveel.
Vereistes	'n Versameling stelsel- of prosesspesifieke vereistes wat deur almal nagekom moet word.
LDAP	*Lightweight Directory Access Protocol*
RADIUS	*Remote Authentication Dial-In User Service*

10. Hersieningsgeskiedenis