UNIVERSITEIT VAN DIE VRYSTAAT

BELEID

| | |
|---|---|
| Dokumentnommer | IS 1000 |
| Dokumentnaam | Beleid oor Inligtingsekuriteit vir Gebruikers van Inligting |
| Dokumenttipe | Ondernemingsbeleid |
| Koördinerende UBK -lid | Senior Direkteur: IKT-dienste |
| Kontak | Bestuurder: Inligtingsekuriteit en Voldoening |
| Status | v2 |
| Goedgekeur deur | UBK |
| Aanvanklike goedkeuring s datum | 19 September 2011 |
| Datum van laaste wysiging | 2 Oktober 2012 |
| Datum wysiging goedgekeur | 18 Februarie 2013 |
| Datum laaste hersien | 2 Oktober 2012 |
| Datum van volgende oorsig | Jaarliks |
| Verwante beleide/wetgewing | · Beleid oor Aanvaarbare Gebruik van Rekenaarhulpbronne<br>· Wet op Elektroniese Kommunikasies en Transaksies, 25 van 2002 |

**INHOUDSOPGAWE**


1. Doel ..... 3
2. Bestek ..... 3
3. Verduidelikende Terme ..... 3
4. Verantwoordelikhede ten opsigte van en Voldoening aan Inligtingsekuriteit ..... 3
5. Prosedures, Standaarde en Riglyne ..... 4
6. Uitsonderings ..... 4
7. Beleidstellings ..... 4
   - 7.1. Inligtingsbeheer en -openbaarmaking ..... 4
   - 7.2. Skoonlessenaar-beleid ..... 4
   - 7.3. Wegdoening met Rekenaarbates en -inligting ..... 5
   - 7.4. Roerende Inligtingsbates ..... 5
   - 7.5. Wagwoorde ..... 5
   - 7.6. Draadlose en Netwerktoegangskoppeling ..... 6
   - 7.7. Afstandstoegang ..... 6
   - 7.8. Sagteware ..... 7
   - 7.9. Antivirus ..... 7
   - 7.10. E-pos ..... 8
   - 7.11. Drukkers ..... 8

## 1. Doel

Die Universiteit van die Vrystaat ("UV") erken 'n verpligting om inligtingsekuriteit vir alle inligtingstegnologiedata, -toerusting en –prosesse in sy domein van eienaarskap en beheer te verseker. Hierdie verpligting word deur elke lid van die Universiteit gedeel.

Hierdie dokument sal die behoefte aan inligtingsekuriteit verduidelik en gepaste vlakke van sekuriteit deur middel van standaarde en riglyne aandui.

## 2. Bestek

Alle gebruikers van inligting is verantwoordelik vir voldoening aan die toepaslike beleide en prosedures.

## 3. Verduidelikende Terme

3.1. **"Moet", "sal", "is verplig"**
Hierdie terme dui 'n verpligte vereiste aan waaraan almal moet voldoen. Die enigste moontlike afwyking is deur middel van 'n formele uitsonderings-vrystelling.

3.2. **"Behoort"**
Hierdie term dui op 'n hoogs aanbevole, maar nie-verpligte, aanbeveling.

3.3. **"Mag", "kan"**
Hierdie terme dui op nie-verpligte aanbevelings.

3.4. **"UV"**
Verwys na die Universiteit van die Vrystaat".

3.5. **"Universiteit"**
Verwys na die Universiteit van die Vrystaat".

3.6. **"Gebruikers"**
Verwys na enige persoon/persone of entiteit(e) wat toegang tot die UV-rekenaarnetwerk of -inligting verkry.

3.7. **"Inligting"**
Verwys na enige inligting of dit nou ook al in geskrewe/gedrukte, verbale of elektroniese vorm is.

## 4. Verantwoordelikhede ten opsigte van en Voldoening aan Inligtingsekuriteit

4.1. Elke gebruiker is verantwoordelik vir sy of haar aksies ten opsigte van die beveiliging van die UV se inligtingsbates.

4.2. Versuim om aan die beleide oor inligtingsekuriteit of ander verwante beleide te voldoen, mag intrekking van die reg om van die stelsels of dienste gebruik te maak en/of dissiplinêre optrede tot gevolg hê.

4.3. Alle vermeende voorvalle met betrekking tot inligtingsekuriteit, -swakhede of -skending moet onmiddellik aan die dienstoonbank van IKT-dienste gerapporteer word.

4.4. Daar word van alle gebruikers van inligting verwag om aan te dui dat hulle hierdie beleid verstaan en aanvaar.

5. Prosedures, Standaarde en Riglyne

5.1. Prosedures, standaarde en riglyne sal as aanhegsels by hierdie beleid gevoeg word en sal 'n integrerende deel van die UV se Beleid oor Inligtingsekuriteit vorm en dit derhalwe in besonderhede omskryf.

6. Uitsonderings

6.1. Uitsonderings ten opsigte van enige beleidstelling moet deur die Senior Direkteur: IKT-dienste goedgekeur word. Alle uitsonderings ten opsigte van beleide sal deur IKT-dienste aangeteken, nagespeur en oorsien word.

7. Beleidstellings

7.1. Inligtingsbeheer en -openbaarmaking

7.1.1. Alle gebruikers moet sorg dra om nie sensitiewe inligting van die UV met ongemagtigde personeel of partye van buite te deel nie.

7.1.2. In geval van inligting wat verlore raak, moet die eienaar van die inligting onmiddellik in kennis gestel word.

7.1.3. Gebruikers moet IKT-dienste in kennis stel van enige probleem ten opsigte van inligtingsekuriteit wat op die netwerk geïdentifiseer is.

7.1.4. Enige personeellid wat toegang benodig tot 'n rekenaar wat nie direk deur hom/haar beheer word nie, moet die toestemming van die eienaar van die rekenaar verkry. Die eienaar van die rekenaar kan beheer oor of toegang tot sy/haar rekenaar skriftelik aan 'n ander personeellid delegeer.

7.1.5. Sensitiewe UV-inligting moet nie op enige derdeparty- wolkgebaseerde stoorfasiliteite gestoor word nie. Wanneer sensitiewe inligting buite die kampus benodig word, moet die UV se SharePoint-fasiliteit gebruik word.

7.2. Skoonlessenaar-beleid

7.2.1. Indien personeellede vir bekende, lang tydperke nie in hulle werkspasies teenwoordig sal wees nie, moet sensitiewe werksdokumente in 'n bêreplek agter slot en grendel, soos 'n laai, geplaas word. As die werkspasie in 'n kantoor geleë is, behoort die kantoordeur gesluit te word.