Universiteit Stellenbosch

Informasiesekuriteitsregulasies

1. Aanhef

1.1. Informasiesekuriteit is 'n komponent van die Risikobestuur-struktuur en -prosedures van die Universiteit.

1.2. Stellenbosch Universiteit is verplig om geskikte sekuriteit vir alle Inligtingstegnologiestelsels (IT-stelsels) - data, toerusting, en prosesse - en informasie wat dit besit en beheer, te verseker. 'n Informasiesekuriteitsregulasie is verpligtend: Elke lid van die universiteit (student en/of personeellid) is in 'n mindere of meerdere mate medeverantwoordelik om geskikte sekuriteit te verseker.

1.3. Geskikte vlakke van sekuriteit moet deur risikobepaling vasgestel word, d.i. bepaling van bedreigings vir, uitwerking op en kwesbaarheid van IT-stelsels en -informasie, asook die waarskynlikheid dat dit kan gebeur.

1.4. Die behoefte aan Informasiesekuriteit word deur drie faktore gedryf:
- 1.4.1. Wetlike, statutêre, regulatoriese en kontraktuele verpligtinge;
- 1.4.2. Risikobepaling;
- 1.4.3. Operasionele beginsels, doelwitte en vereistes vir informasiestelsels wat die Universiteit bepaal of ontwikkel het.

2. Die Rektor se Bestuurspan erken en bevestig die belangrikheid van Informasiesekuriteit en die noodsaaklikheid om informasiesekuriteitsrisiko's te verminder.

3. Dit is die verantwoordelikheid van die Senior Direkteur: Informasietegnologie om:

3.1. Beleid, regulasies, standaarde, riglyne en organisasie te ontwikkel en te implementeer, en die verantwoordelikhede te delegeer wat nodig is om die Universiteit se informasiesekuriteitsrisiko's (aanvullende regulasies wat omvang, organisasie en rolle uiteensit, word in Bylae A beskryf) te verminder.

3.2. Leierskap, verantwoordelikheid en beheer van reaksies op informasiesekuriteitsinsidente, -bedreigings en -oortredings te aanvaar.

4. Definisie van Informasiesekuriteit[1].

4.1. Sekuriteit kan gedefinieer word as " 'n toestand sonder onaanvaarbare risiko's". Die risiko's kan binne die volgende kategorieë van moontlike verliese beskou word:

4.1.1. *Vertroulikheid* van informasie. Vertroulikheid beteken om seker te maak dat informasie slegs toeganklik is vir diegene wat daartoe gemagtig is.

4.1.2. *Integriteit* van informasie en verwerking. Integriteit beteken om die akkuraatheid en volledigheid van informasie en verwerkingsmetodes te beveilig.

4.1.3. *Beskikbaarheid van stelsel.* Beskikbaarheid beteken om seker te maak dat gemagtigde gebruikers toegang tot informasie en verwante bates het wanneer nodig.

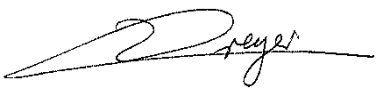
4.1.4. *Bates.* Die bates wat die Universiteit besit en/of beheer wat beskerm moet word, sluit die volgende in:

4.1.4.1. Rekenaar en randtoerusting;
4.1.4.2. Kommunikasietoerusting;
4.1.4.3. Rekenaar- en kommunikasieperseel;
4.1.4.4. Krag, water, omgewingsbeheer en kommunikasie-benodigdhede;
4.1.4.5. Voorrade en databergingsmedia;
4.1.4.6. Stelselrekenaarprogramme en -dokumentasie;
4.1.4.7. Toepassingsrekenaarprogramme en -dokumentasie;
4.1.4.8. Informasie.

4.1.5. *Doeltreffende en geskikte gebruik.* Doeltreffende en geskikte gebruik verseker dat die Universiteit se informasiestelselbates met die oogmerk gebruik word waarvoor dit bedoel is, op so 'n manier (d.i. doeltreffende, nie verkwistende nie, gebruik van hulpbronne soos geheuekapasiteit, bandwydte en verwerkingstyd) dat daar nie inbreuk gemaak word op ander se redelike toegangsregte nie.

4.2. Die potensiële oorsake van hierdie verliese word "bedreigings" genoem. Hierdie bedreigings kan menslik of nie-menslik wees, natuurlik, toevallig of doelbewus.

5. Hierdie is interim regulasies en sal deur 'n Informasiesekuriteits-beleid vervang word.

Geteken:  Geteken: 

RF Pina, Direkteur IT: E-besigheid MW Dreijer, Senior Direkteur: IT

Geteken namens die Rektor se Bestuurspan:

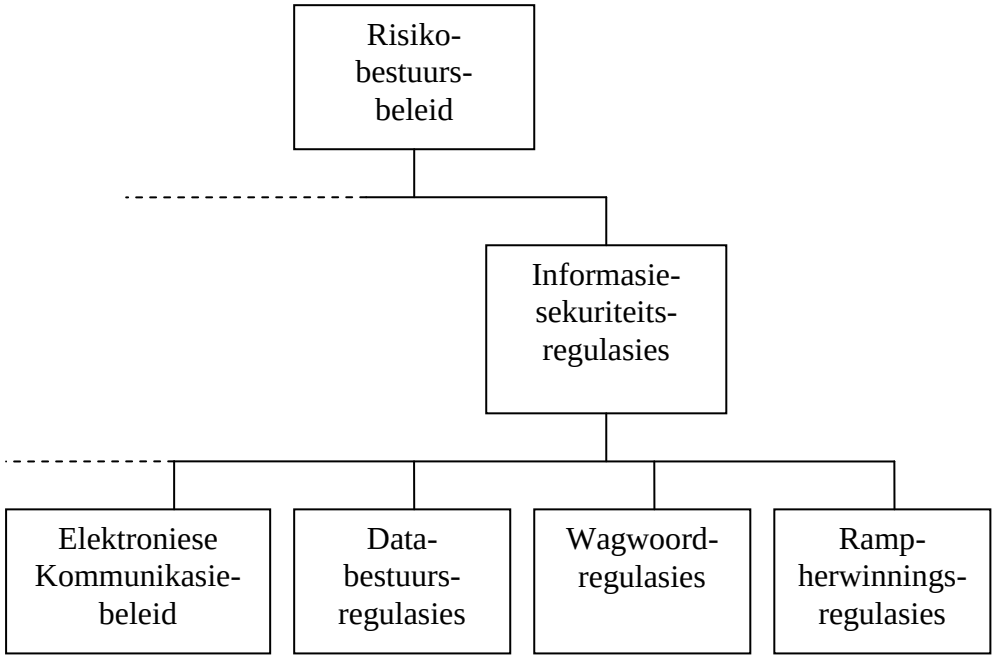
Prof L van Huyssteen, Uitvoerende Direkteur: Bedryf en Finansies: 4 Okt 2010

[1] Ons bedank graag die Murdoch Universiteit, Australië, vir die toestemming vir die gebruik van elemente van hul Informasiesekuriteitsbeleid in die opstel van hierdie regulasie.

BYLAE A: Informasiesekuriteit: omvang, rolle en organisasie

1. Dokumenthiërargie

1.1. Die Informasiesekuriteitsregulasies sal met bestaande en ontwikkelende beleid/regulasies oorvleuel (bv. Elektroniese Kommunikasiebeleid, Rampherwinningsregulasie, Privaatheidsbeleid, Databestuurregulasies, ens. soos toepaslik. Verwys na Figuur 1: Hiërargie vir Informasiesekuriteitsbeleid/regulasiedokument). Wanneer dit gebeur, sal hierdie regulasie voorkeur geniet, 'n kruisverwysingsraamwerk verskaf en na die ander beleid/regulasies verwys waar toepaslik.



Figuur 1: Hiërargie vir Informasiesekuriteitsbeleid/regulasie dokumente

2. Die omvang van Informasiesekuriteit

2.1. In aansluiting by die definisie van informasiesekuriteit soos hierbo uiteengesit, word die volgende domeine en raamwerke beskryf:

2.2. Informasiesekuriteitsdomeine en -raamwerke

Beleid en regulasies wat kragtens hierdie beleid gepromulgeer word, moet binne die volgende domeine en raamwerke gestruktureer word:

2.2.1. **Bestuursekuriteit**

Rolle en organisasiestruktuur word in die volgende afdeling beskryf.

Administratiewe sekuriteit: Dit sluit in: Gebruikersopleiding en -bewustheid; rapportering van sekuriteitsprobleme; kontroles en risikobepaling; uitkontraktering en derdepartykontrakte.
Menslike hulpbronne en Studentesake: Dit sluit in: Dissipline en gevolge; kwalifikasies en vaardighede; rugsteunpersoneel; agtergrondverifikasie.
Besigheidskontinuïteitsbestuur: Dit sluit in: Rampherwinnings-beplanning, gebeurlikheidsbeplanning; toets van planne; identifikasie en vermindering van risiko's.

2.2.2. **Logiese sekuriteit**

Programmatuursekuriteit: Dit sluit in: Stelseltoegangsbeheer en wagwoordbestuur; voorregtebeheer en boekstawing.
Programmatuurontwikkeling en veranderingsbeheer: Dit sluit in: Hantering van virusse en wurms; die programmatuurontwikkelings-proses; die veranderingsbeheerproses, ook vir werkstasies; derdepartybetrokkenheid.
Datasekuriteit: Dit sluit in: intellektuele-eiendomsreg; dataprivaatheid; datavertroulikheid; datakritikaliteit en data-integriteit.
Kommunikasiesekuriteit: Dit sluit in: Die daarstel van netwerkkonneksies; vloeibeheerstelsels insluitend netskans ('firewall'), enkripsie, skakelkommunikasie ('dial-up communication'); afgelaaide data; telefoonstelsels; elektronieseposstelsels; reëlings vir mense wat van die huis af werk ('telecommuting arrangements'); internetverbindings en elektroniese betaalstelsels.

2.2.3. **Fisiese sekuriteit**

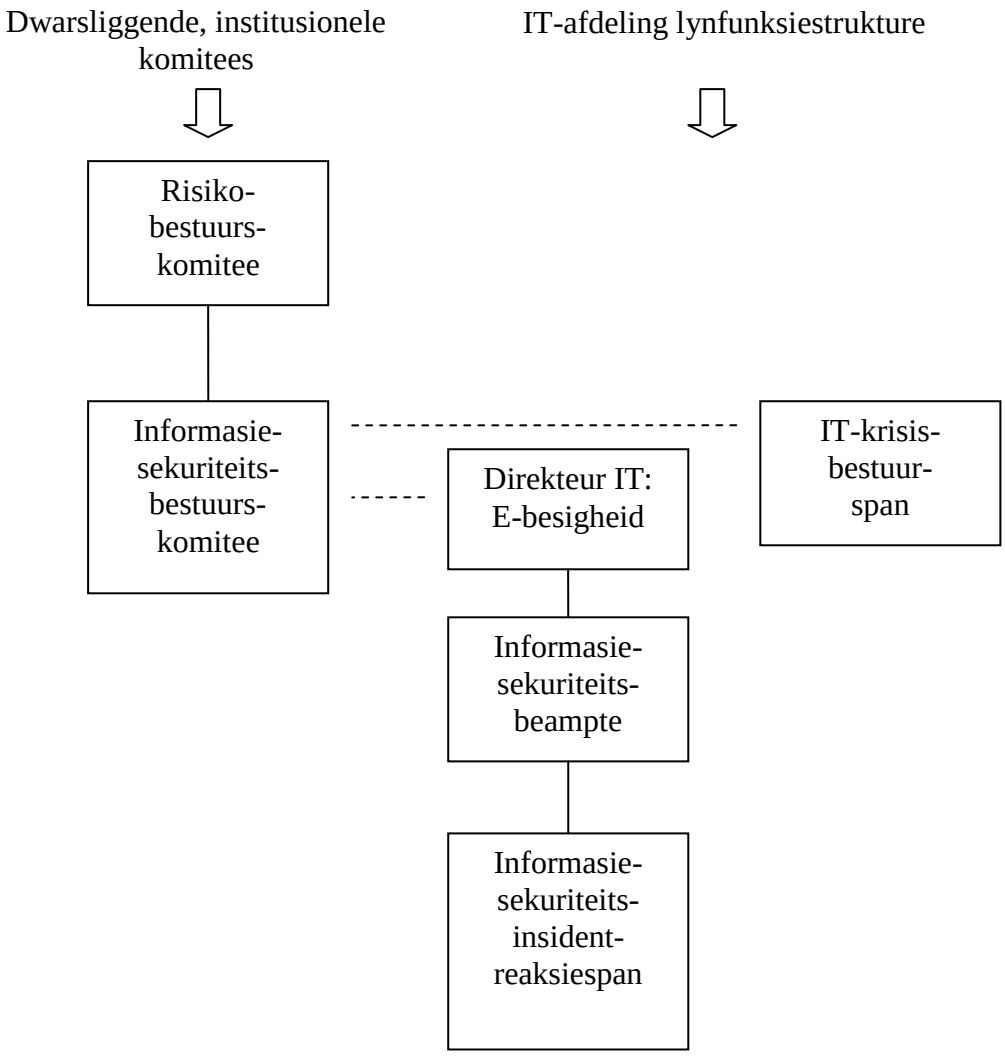
Fisiesetoegangsekuriteit: Dit sluit in: Toegangsbeheer na geboue en rekenaarfasiliteite.
Rekenaarlokalisering en -omgewing: Dit sluit in: Die perseel; datasentrumperseel in geval van nood; konstruksie; kragtoevoer; noodtoerusting; alarmstelsels; gebeurlikheidsplanne, ens.

3. Rolle en organisasiestruktuur

3.1. Regulasiebestuur

Die volgende organisasiestruktuur (Verwys na Figuur 2: Organogram vir Informasiesekuriteit) word buiten die bestaande lynbestuurstrukture omskryf om Informasiesekuriteit op 'n dwarsliggende en institusionele wyse te bestuur, reguleer en te implementeer:

- 'n Informasiesekuriteitsbestuurkomitee, onder die voorsitterskap van die Senior Direkteur: Informasietegnologie as Hoofinligtingsbeampte (HIB), wat as 'n subkomitee van die Risikobestuurkomitee funksioneer;
- 'n Informasiesekuriteitsinsident-reaksiespan;
- 'n Informasiesekuriteitsbeampte.



Figuur 2: Organogram vir Informasiesekuriteit

3.1.1. Informasiesekuriteitsbestuurkomitee

Die funksies van hierdie multidissiplinêre, institusionele komitee is om:

- Die Informasiesekuriteitsregulasies, ondergeskikte beleid en regulasies wat kragtens die Informasiesekuriteitsregulasies ontwikkel is en die jaarlikse Informasiesekuriteitsplan te ondersoek en goed te keur;
- Informasiesekuriteitsverantwoordelikhede te bepaal en verantwoordelike persone in Informasiesekuriteitsrolle deur die instelling aan te wys;
- Groot sekuriteitsinsidente te ondersoek en te monitor.
- Betekenisvolle veranderinge in die blootstelling van IT-bates aan ernstige bedreigings te monitor;
- Gereelde risikobepalings te inisieer en te ondersoek;
- Aan die Risikobestuurskomitee oor Informasiesekuriteiskwessies te rapporteer;

- Die Uitvoerende Bestuur oor Informasiesekuriteitskwessies te adviseer.

Die Informasiesekuriteit-bestuurskomitee sal uit ten minste die volgende bestaan[2]:

- Die Senior Direkteur: IT (Voorsitter);
- 'n Verteenwoordiger van die Interne Ouditkomitee;
- Die Hoof Direkteur: Finansies of 'n afgevaardigde;
- Die Hoof: Beskermingsdienste of ‘n afgevaardigde;
- Die Hoof Direkteur: Menslike Hulpbronne of 'n afgevaardigde;
- Die Senior Direkteur: Institusionele Navorsing en Beplanning of ‘n afgevaardigde;
- Die Hoof: Regsdienste of ‘n afgevaardigde;
- Die Registrateur of ‘n afgevaardigde;
- Die Senior Direkteur: Navorsingsonwikkeling of ‘n afgevaardigde;
- ‘n Akademiese personeellid van die Departement Inligtingskunde;
- 'n Verteenwoordiger van die Studenteraad;
- Die Informasiesekuriteitsbeampte, as verteenwoordiger van die Informasiesekuriteitsinsident-reaksiespan;
- Die Direkteur IT: E-besigheid (Koördineerder).

Die komitee moet ten minste elke kwartaal vergader.

3.1.2. Informasiesekuriteitsinsident-reaksiespan[3]

Die Informasiesekuriteitsinsident-reaksiespan sal verkieslik die volgende dienste in die volgende dienskategorieë verskaf:

Reaktiewe dienste: Dienste wat deur 'n gebeurtenis of rapportering veroorsaak word:

- Verspreiding van alarmsein en waarskuwings;
- Hantering van insidente;
- Hantering van kwesbare plekke;
- Hantering van artefakte[4].

Proaktiewe dienste: Dienste wat hulp en informasie verskaf om, in afwagting van bedreigings, te help voorberei, beskerm en bates te beveilig :

- Aankondigings;

[2] Dit word nie vereis dat die komitee verteenwoordigend moet wees nie, maar eerder dat die lede oor die vereiste kennis beskik om tot die institusionele bestuur van informasiesekuriteit ‘n bydrae te kan maak.

[3] Die Insidentreaksiespan moet nie verwar word met die IT-krisisbestuurspan wat geskep is kragtens die IT-krisisbestuurplan nie. Laasgenoemde bestaan uit die IT-Senior Direkteur en -Direkteure en sal bepaal wanneer 'n Informasiesekuriteitsinsident tot 'n IT-krisis eskaleer.

[4] Lêers of voorwerpe wat op 'n stelsel gevind word wat betrokke kan wees in die deurdring, aanval of mislei van sekuriteit op stelsels. Dit kan virusse, Trojaanse perdprogramme, eksploiteringsteks, wurms of ’n stel hulpmiddels (*toolkit*) wees.

- Sekuriteitsoudits en -bepalings;
- Tegnologiewagdiens;
- Riglyne oor konfigurasie en onderhoud van sekuriteitshulpmiddels, -toepassings, -infrastruktuur en -dienste;
- Voorbereiding en formulering van gedetailleerde sekuriteitsregulasies, -riglyne en -standaarde as deel van die Informasiesekuriteisregulasies. Sodanige dokumente moet aan die Direkteur IT: E-besigheid voorgelê word vir verdere bestuursondersoek en -goedkeuring waar nodig;
- Voorbereiding van 'n jaarlikse Informasiesekuriteitsplan;
- Indringer-opsporingsdienste;
- Verskaf 'n sekuriteitsverwante informasiestoor.

Sekuriteitskwaliteitsbestuurdienste: Hulp met:

- Risiko-analise;
- Voortsetting van besigheid en rampherwinningsbeplanning;
- Sekuriteitskonsultering;
- Bewusmaking;
- Opvoeding en opleiding;
- Produkevaluering of -sertifisering.

Die Informasiesekuriteitsinsident-reaksiespan sal bestaan uit:

- Die Informasiesekuriteitsbeampte, wat voorsitter van formele vergaderings sal wees en die span sal koördineer;
- Alle Stelsel- en Databasisadministrateurs in die IT-afdeling;
- Alle Stelsel- en Databasisadministrateurs in afdelings en fakulteite wat nie aan die IT-afdeling rapporteer nie, soos benodig;
- Rekenaargebruiksarea-bestuurders soos benodig;
- Die Bestuurder: IT-steundienste;
- 'n Kommunikasie-/mediaspesialis, soos benodig;
- Gekoöpteerde tegniese spesialiste, soos benodig.

3.1.3. Informasiesekuriteitsbeampte

Die Informasiesekuriteitsbeampte is 'n tegniese sekuriteitsdeskundige wat verantwoordelik is vir die volgehoue bestuur van die informasiesekuriteitsregulasies, -standaarde, -prosedures en -tegniese stelsels. As sodanig is 'n sleutelprestasiegebied (SPG) van die pos die koördinering van die Informasiesekuriteitsinsident-reaksiespan. Die posisie moet verkieslik 'n nuwe en aparte pos wees, maar die SPGs moet realisties gedelegeer word aan 'n bestaande posisie binne die IT-afdeling.

3.2. Kuratorskap en gebruikerverantwoordelikhede

Die kurator van 'n informasiebate sal verantwoordelik wees vir die Informasiesekuriteit daarvan.

3.2.1. Kurators[5]

- Die IT-afdeling (IT) sal die kurator van alle strategiese stelselplatforms en -infrastruktuur wees;
- IT sal die kurator wees van die strategiese kommunikasiestelsels;
- Dekane sal die kurators wees van rekenaarlaboratoriums/ rekenaargebruiksareas (RGAs) in hul onderskeie besit;
- Afdelings, departemente en eenhede sal die kurators wees van strategiese *applikasies en informasie* onder hulle bestuursbeheer (bv. Finansies, Menslike Hulpbronne, Sentrum vir Onderrig en Leer, Biblioteek);
- Dekane en hoofde van afdelings, departemente, institute en eenhede sal kurators wees van alle nie-strategiese stelsels in hulle besit;
- Individue sal kurators wees van lessenaarstelsels (*desktop systems*) onder hulle beheer.

3.2.2. Gebruikers

- Elke gebruiker van die Universiteit se informasiehulpbronne, insluitend alle personeel en studente, sal verantwoordelik wees om aan gedragstandaarde te voldoen wat kragtens hierdie regulasie bekend gemaak word.
- Alle gewone gebruikers van die Universiteit se informasiehulpbronne:
  - Sal die beleid, regulasies, riglyne, standaarde en praktykkodes soos van tyd tot tyd kragtens hierdie regulasie gepromulgeer word, nakom;
  - Is verantwoordelik vir die behoorlike versorging en gebruik van informasiehulpbronne onder hulle direkte beheer;
  - Is verplig om sekuriteitsinsidente aan die IT-Hulptoonbank of die relevante RGA-bestuurders te rapporteer;
  - Moet vereiste rekenaarsekuriteits- en funksionele opleiding bywoon.
- Alle spesiale tipe gebruikers van die Universiteit se IT-hulpbronne soos kontrakteurs, konsultante, genote, besoekende personeel, besoekers, ens.:
  - Moet die beleid, riglyne, standaarde en praktykkodes soos van tyd tot tyd kragtens hierdie regulasie gepromulgeer word, nakom;
  - Is verantwoordelik vir die behoorlike versorging en gebruik van informasiehulpbronne onder hulle direkte beheer;

[5] Kurators beskerm en sorg vir die bates onder hulle sorg.

- Is verplig om sekuriteitsinsidente aan die IT-Hulptoonbank of die relevante RGA-bestuurders te rapporteer.

Bogenoemde voorwaardes moet in die standaardterme en -voorwaardes ingesluit word wat deel is van die kontrakte en ooreenkomste wat die verhoudings tussen sodanige gebruikers en die Universiteit beheer.

'n Gereelde oudit van informasiebates moet onderneem word, die kurators (en hul afgevaardigde bestuurders) moet geïdentifiseer word en hulle verantwoordelikhede moet gedokumenteer word.

4. Regulasiehersiening en onderhoudsiklus

Hersiening van die Informasiesekuriteitsregulasies sal deur die gereelde risikobepalings wat deur die Informasiesekuriteit-bestuurskomitee geïnisieer en gedryf word, of wanneer die Komitee besluit dat 'n hersiening nodig is as gevolg van veranderinge in die omgewing.

Die Informasiesekuriteitsinsident-reaksiespan sal ten minste een keer per maand bymekaar kom en sal beleidveranderings aan die Informasiesekuriteit-bestuurskomitee voorstel waar nodig. Dit sal egter gedetailleerde beleid, regulasies, standaarde, planne en riglyne deurlopend hersien en aanpas.