NWU Beleid en Reëls oor Data- en Inligtingsekuriteit

Verwysingsnommer	1P_1.16.1_a
Verantwoordelike uitvoerende bestuurder	Registrateur
Beleideienaar	Registrateur
Verantwoordelike afdeling	Kantoor van die Registrateur
Status	Goedgekeur
Goedgekeur deur	Raad
Datum van goedkeuring	23 Junie 2022
Datum van wysigings	
Hersieningsdatum	2025

Kantoor van die Registrateur

NWU BELEID EN REËLS OOR DATA- EN INLIGTINGSEKURITEIT

Aanhef

Teen die agtergrond van die droom om 'n internasionaal erkende universiteit in Afrika te wees, wat bekend is vir sy wetenskapsbeoefening, maatskaplike responsiwiteit en 'n sorgsaamheidsetiek, het die Raad van die Noordwes-Universiteit (NWU) die Beleid en Reëls oor Data- en Inligtingsekuriteit op 23 Junie 2022 aanvaar.

1 Vertolking en toepassing

Hierdie beleid moet vertolk en toegepas word op 'n wyse wat strook met die –

1.1 Grondwet van die Republiek van Suid-Afrika, 1996;

1.2 Wet op Hoër Onderwys, 101 van 1997;

1.3 Wet op die Beskerming van Persoonlike Inligting, 4 van 2013 ("WBPI");

1.4 Wet op die Bevordering van Toegang tot Inligting, 2 van 2000 ("WBTI");

1.5 King IV-verslag oor Korporatiewe Bestuur in Suid-Afrika;

1.6 WBPI-industriegedragskode: Openbare Universiteite (USAf, Junie 2020);

1.7 Statuut van die Noordwes-Universiteit ("die Statuut");

1.8 Inligtingsbestuursraamwerk van die NWU;

1.9 Die NWU se Risikobestuursbeleid;

1.10 Die NWU se Besigheidskontinuïteitsbeleid;

1.11 Die NWU se IT-korporatiewebestuursbeleid;

1.12 Die NWU se IT-beleid oor Billike Gebruik; en

1.13 Reëls en Riglyne m.b.t. IT en inligtingsekuriteit soos van tyd tot tyd gepubliseer deur die Universiteit.

2 Begripsomskrywings

In hierdie beleid –

beteken **"data"** die voorstelling van feite, konsepte of instruksies op 'n formele wyse, geskik vir kommunikasie, vertolking of verwerking deur mense óf outomaties; en

beteken **"inligting"** kennis aangaande voorwerpe soos feite, gebeure, dinge, prosesse of idees, insluitend konsepte wat 'n bepaalde betekenis binne 'n sekere konteks het.

3 Beleidsverklaring

3.1 Die NWU beskou data- en inligtingsekuriteit as van kardinale belang vir die goeie korporatiewe bestuur en die effektiewe en doeltreffende bestuur en administrasie van die Universiteit.

3.2 Die reëls soos uiteengesit in paragraaf 5 word aanvaar om die data- en inligtingsekuriteit van die Universiteit teen alle bedreigings te handhaaf.

4 Omvang van toepassing

Hierdie beleid en die reëls uiteengesit in paragraaf 5 is van toepassing op sekuriteitsmaatreëls in die generering, bestuur en byhou van alle soorte data en inligting by die NWU aangesien dit in alle besigheidsprosesse en deur alle lede van die NWU, sy verskaffers en diensverskaffers plaasvind.

5 Reëls oor data- en inligtingsekuriteit

5.1 Vir die doeleindes van die implementering van ’n algehele en eenvormige data- en inligtingsekuriteitbestuurstelsel moet die volgende oorkoepelende doelwitte nagestreef word:

5.1.1 die ontwikkeling en instandhouding van ’n gedetailleerde data- en inligtingstelsel-inventaris, wat volledige inligting bevat oor al die IT-stelsels wat by die NWU gebruik word;

5.1.2 die kategorisering van data- en inligtingstelsels ten opsigte van vlakke van vertroulikheid, integriteit en beskikbaarheid, elk gegradeer in ooreenstemming met die sensitiwiteit van data wat dit bevat en met betrekking tot die vereiste sekuriteitsmaatreëls wat nodig is om die data en inligting te beskerm, en

5.1.3 die bestuur van data- en inligtingsekuriteit op ’n proaktiewe wyse om risiko’s, uitdagings en bedreigings in die institusionele netwerk soos interne en eksterne kuberaanvalle en stelselwanfunksionering en verlies van data te beperk.

5.2 ’n Bestuur- en bestuursomgewing wat bevorderlik is vir die implementering van inligtingsekuriteitskontroles wat die NWU se data en sy inligtingsbates beskerm, moet daargestel en in stand gehou word –

5.2.1 deur middel van ’n sistematiese en deurlopende ondersoek van data- en inligtingsekuriteitsrisiko’s relevant tot hoër onderwys in die algemeen en die NWU in die besonder, met inagneming van eksterne bedreigings, inherente kwesbaarhede en die impak van risiko’s relevant tot data- en inligtingsekuriteit;

5.2.2 deur ’n stelselsekuriteitsplan te ontwikkel en in stand te hou wat risiko’s met betrekking tot data- en inligtingsekuriteit uiteensit, die vereiste kontroles en voorsiening van gerusstelling, met inbegrip van sekuriteitsbeplanning deur middel van ’n omvattende gehaltebestuursbenadering, wat van die Beplan-Doen-Nagaan-Optree-model afwyk ten einde toereikende dekking van die sekuriteitsbestuurlewensiklus te verseker:

- Beplan: gedokumenteerde riglyne, prosedures relevant tot sekuriteitsdoelwitte, padkaarte om dit te bereik, insluitende moniteringsmeganismes en verantwoordelikheidsmatrikse.
- Doen: implementering van sekuriteitskontroles.
- Nagaan: uitvoering van toetse om te bepaal dat kontroles werk soos bedoel en dat dit aan die vereiste doelwitte voldoen.
- Optree: Remediëring van leemtes en tekortkominge.

5.2.3 deur ’n konfigurasiebestuursomgewing daar te stel met die doel om ’n volledige begrip te verskaf van die NWU se data- en inligtingslandskap ten opsigte van sy netwerktoestelle, bedryfstelsels, toepassings, ekstern en intern ontwikkelde dienste, stelsels, hardeware- en sagtewareplatforms ten einde die sekuriteit van hierdie konfigurasies daar te stel, in stand te hou en te moniteer.

5.2.4 Deur stelsel-, data- en inligtingintegriteit te verseker deur die daarstelling van relevante maatreëls, insluitend dié wat verband hou met indringerware, toepassings- en bronkodefoute, veiligheidswaarskuwingsadvies en -riglyne, gemorsposbeskerming, inligtinginvoervalidering, sowel as die herstel van bespeurde en geopenbaarde integriteitskwessies;

5.2.5 Deur die implementering en bestuur van beheermaatreëls voor, tydens en na ’n kontraktuele verhouding tussen die NWU en enige individu of party;

5.2.6 Deur die implementering van ’n voorval-reaksie-struktuurplan om toepaslike reaksies en deurlopende verbetering te verseker op vlakke waar data- en inligtingsekuriteitvoorvalle plaasvind, wat die volgende aandui op die relevante vlak van bedryf:

- die verantwoordelikheidsmatriks
- prosedures wat geïmplementeer moet word
- reaksie- en hersteltyd m.b.t. voorvalle
- getuienis
- leer uit voorval

5.2.7 deur middel van die identifisering van en verifikasie rakende aspekte wat relevant is om gereedheid, prestasie, ontwerp en implementering van sekuriteitsmaatreëls vir sakebedrywighede sowel as met betrekking tot besigheidskontinuïteit te verseker;

5.2.8 deur toegangsbeheer tot data en inligting en fisiese liggings te bestuur, dit wil sê die verskaffing van riglyne en prosedures wat digitale en fisiese toestemmingsbeperkings definieer ten opsigte van aangeleenthede wat verband hou met data- en inligtingsklassifikasie in ooreenstemming met paragraaf 5.1.2, en in ooreenstemming met die NWU-lêerplan;

5.2.9 deur toegangsregte tot fisiese ruimtes te bestuur, asook toegangsbeheer tot netwerke en netwerkdienste;

5.2.10 deur bewusmakings- en opleidingsprogramme te implementeer wat gerig is op die relevante interne en eksterne belanghebbendes oor aangeleenthede met betrekking tot data- en inligtingsekuriteit, die implementering van hierdie beleid, en deur praktiese maatreëls te tref wat die doeltreffendheid van die inligtingsekuriteitsmaatreëls demonstreer;

5.2.11 deur 'n oorkoepelende besigheidskontinuïteitsraamwerkplan te implementeer wat bestaan uit 'n reeks planne, prosedures, tegniese vereistes en inisiatiewe om die herstel van inligtingstelsels, bedrywighede, data en inligting in alle gevalle van ontwrigting van relevante dienste te verseker;

5.2.12 deur deurlopende inligtingsekuriteitsprestasie en verwante prosesse te moniteer en daaroor verslag te doen, met inbegrip van beheermaatreëls met die doel om deurlopende kwaliteitsverbetering en rypheidsvlakke te verseker, ten einde onder meer die volgende te bepaal:

5.2.12.1 besigheidsprosesse en resultate wat deur variasies ten opsigte van inligtingsekuriteitsprestasie beïnvloed kan word, insluitend die kontroles wat relevant is in sulke omgewings, sowel as relevante gevalle van regulatoriese en riglynebestuur; en

5.2.12.2 metodes wat gebruik moet word vir doeleindes van meting in die betrokke omgewing (insluitend handleiding, meganies, sagteware) om verifieerbare en herhaalbare resultate te verseker;

5.2.13 deur versekering te verskaf oor die toepaslikheid, die effektiwiteit en doeltreffendheid van inligtingsekuriteitskontroles wat die Universiteit se data- en inligtingsbates beskerm; en

5.2.14 deur bewyse en verslae te verskaf wat vir ouditspoor- en bestuursdoeleindes opgestel is.

6 Rolle, verantwoordelikhede en aanspreeklikheid

6.1 Die Raad is aanspreeklik en neem verantwoordelikheid vir die daarstelling van 'n omgewing wat bevorderlik is vir die korporatiewe bestuur van effektiewe en doeltreffende data- en inligtingsekuriteitbestuur.

6.2 Die Raad word deur die Komitee vir Korporatiewe Bestuur van IT (TIGovCom) geadviseer oor die wyse waarop hierdie beleid geïmplementeer word, oor die toepaslikheid van die riglyne, reëls, prosedures en protokolle ten opsigte van die NWU se data- en inligtingsekuriteitbestuurstelsel en die doeltreffendheid van die bestuur van relevante risiko's.

6.3 Die Universiteitsbestuurskomitee (UMK) is verantwoordelik vir die daarstelling van 'n bestuursomgewing om data- en inligtingsekuriteit in alle besigheidsprosesse te verseker en vir die bereiking van die bestuursdoelwitte wat die Raad in ooreenstemming met hierdie beleid gestel het.

6.4 Die UBK moet –

6.4.1 'n kultuur bevorder wat data- en inligtingsekuriteit in alle relevante besigheidsprosesse inbed;

6.4.2 riglyne, reëls, standaarde en prosedures ten opsigte van 'n oorkoepelende NWU-data- en inligtingsekuriteitbestuurstelsel daarstel;

6.4.3 die implementering van 'n program verseker om deurlopende bewustheid en opleiding van alle interne belanghebbendes te verseker in sake relevant tot data- en inligtingsekuriteit; en

6.4.4 verslag doen oor die doeltreffendheid en effektiwiteit van die implementering van die NWU se data- en inligtingsekuriteitbestuurstelsel aan die TIGovCom.

Met betrekking tot die deurlopende bestuur van aangeleenthede wat verband hou met data- en inligtingsekuriteit, ontvang die Inligtingsbestuurskomitee (IMCom) en die Inligtingstegnologiekomitee (ITCom) verslae van die Registrateur se portefeulje en van die Hoofdirekteur IT en adviseer die UBK oor die effektiewe en doeltreffende bestuur van data- en inligtingsekuriteit in ooreenstemming met hierdie beleid.

Oorspronklike gegewens: (11664754) P:\Policies\2022\1P_1.16.1A\NWU Beleid en Reëls oor Data- en Inligtingsekuriteit.docm
7 Julie 2022

Verwysingsnommer: 1P_1.16.1_A